POLÍTICA DE CERTIFICACIÓN DE LA INFRAESTRUCTURA DE CLAVE PÚBLICA DEL PARAGUAY

Ministerio de Industria y Comercio

Subsecretaría de Estado de Comercio

República del Paraguay

Tabla de contenido

1.1 Descripción general 1

1.2 Nombre e Identificación del documento 3

1.3 Participantes de la PKI 3
1.3.1 Autoridades Certificadoras (CA) 3
1.3.2. Autoridad de Registro (RA) 3
1.3.3. Suscriptores 4
1.3.4. Parte que confía 4
1.3.5. Otros participantes 4

1.4 Uso del Certificado 4
1.4.1 Usos apropiados del Certificado 5
1.4.2. Usos prohibidos del certificado 6

1.5 Administración de la Política 6
1.5.1. Organización que administra el documento 6
1.5.2. Persona de Contacto 6
1.5.3. Persona que determina la adecuación de la CPS a la Política 7
1.5.4 Procedimientos de aprobación de la Política de Certificación (CP) 7
1.6 Definiciones y acrónimos 7
1.6.1 Definiciones 7
1.6.2 Acrónimos 13

2 RESPONSABILIDADES DE PUBLICACION Y DEL REPOSITORIO 15
2.1. Repositorios 15
2.2 Publicación de Información de Certificación 15
2.3 Tiempo o frecuencia de Publicación 16
2.4 Controles de Acceso a los Repositorios 16

3 IDENTIFICACION Y AUTENTICACION 16
3.1 Nombres 16

3.1.1 Tipos de Nombres 16
3.1.2. Necesidad de Nombres significativos 20
3.1.3. Anonimato o seudónimos de los suscriptores 20
3.1.4 Reglas para interpretación de varias formas de Nombres 20
3.1.5 Unicidad de los nombres 21
3.1.6 Reconocimiento, autenticación y rol de las marcas registradas 21
3.2 Validación inicial de identidad 21
3.2.1 Método para probar posesión de la clave privada 22
3.2.2 Autenticación de identidad de Persona Jurídica 22
3.2.3 Autenticación de identidad de Persona Física 22
3.2.4 Información del Suscriptor no verificada 22
3.2.5. Validación de la Autoridad (Capacidad de hecho) 23
3.2.6. Criterios para interoperabilidad 23
3.3 Identificación y autenticación para solicitudes de re emisión de claves 23
3.3.1 Identificación y autenticación para re emisión de claves rutinaria 23
3.3.2 Identificación y autenticación para la re emisión de claves después de una revocación 23
3.4 Identificación y autenticación para solicitudes de revocación 24

4 REQUERIMIENTOS OPERACIONALES DEL CICLO DE VIDA DEL CERTIFICADO 24

4.1 Solicitud del Certificado 24
4.1.1 Quién puede presentar una solicitud de certificado 24
4.1.2 Proceso de Inscripción y responsabilidades 25
4.2. Procesamiento de la Solicitud del Certificado 27
4.2.1 Ejecución de las funciones de Identificación y Autenticación 27
4.2.2 Aprobación o rechazo de solicitudes de certificado 27
4.2.3. Tiempo para procesar solicitudes de Certificado 27
4.3 Emisión del Certificado 28
4.3.1 Acciones de la CA durante la emisión de los certificados 28
4.3.2 Notificación al suscriptor sobre la emisión del Certificado Digital 28
4.4. Aceptación del Certificado 29
4.4.1 Conducta constitutiva de aceptación de certificado 29
4.4.2 Publicación del Certificado por la CA 29
4.4.3 Notificación de la emisión del certificado por la CA a otras entidades 29
4.5 Uso del par de claves y del certificado 29
4.5.1 Uso de la Clave privada y del certificado por el Suscriptor 29
4.5.2 Uso de la clave pública y del certificado por la parte que confía 31
4.6 Renovación del certificado 31
4.6.1 Circunstancias para renovación de certificado 32
4.6.2 Quién puede solicitar renovación 32
4.6.3 Procesamiento de solicitudes de renovación de certificado 32
4.6.4 Notificación al suscriptor sobre la emisión de un nuevo certificado 32
4.6.5 Conducta constitutiva de aceptación de un certificado renovado 32
4.6.6 Publicación por la CA del certificado renovado 32
4.6.7 Notificación por la CA de la emisión de un certificado a otras entidades 32
4.7 Re-emisión de claves de certificado 32
4.7.1 Circunstancias para re-emisión de claves de certificado 33
4.7.2 Quien puede solicitar la certificación de una clave pública 33
4.7.3 Procesamiento de solicitudes de re-emisión de claves de certificado 33
4.7.4 Notificación al suscriptor sobre la re-emisión de un nuevo certificado 33
4.7.5 Conducta constitutiva de aceptación de un certificado re-emitido 33
4.7.6 Publicación por la CA de los certificados re-emitidos 33
4.7.7 Notificación por la CA de la re-emisión de un certificado a otras entidades 33

4.8 Modificación de certificados 33
4.8.1 Circunstancias para modificación del certificado 33
4.8.2 Quién puede solicitar modificación del certificado 34
4.8.3 Procesamiento de solicitudes de modificación del certificado 34
4.8.4 Notificación al suscriptor de la emisión de un nuevo certificado 34
4.8.5 Conducta constitutiva de aceptación del certificado modificado 34
4.8.6 Publicación por la CA de los Certificados modificados 34
4.8.7 Notificación por la CA de emisión de certificado a otras entidades 34
4.9 Revocación y suspensión 34
4.9.1 Circunstancias para la revocación 34
4.9.2 Quien puede solicitar Revocación 36
4.9.3 Procedimiento para la solicitud de revocación 36
4.9.4 Periodo de gracia para solicitud de revocación 37
4.9.5 Tiempo dentro del cual la CA debe procesar la solicitud de revocación 37
4.9.6 Requerimientos de verificación de revocación para las partes que confían 37
4.9.7 Frecuencia de Emisión del CRL 37
4.9.8 Latencia máxima para CRLs 38
4.9.9 Disponibilidad de verificación de revocación/ estado en línea 38
4.9.10 Requerimientos para verificar la revocación en línea 38
4.9.11 Otras formas de advertencias de revocación disponibles 38
4.9.12 Requerimientos especiales por compromiso de clave privada 38
4.9.13 Circunstancias para suspensión 39
4.9.14 Quien puede solicitar la suspensión 39
4.9.15 Procedimiento para la solicitud de suspensión 39
4.9.16 Límites del período de suspensión 39
4.10 Servicios de comprobación de estado de Certificado 39
4.10.1 Características operacionales 39
4.10.2 Disponibilidad del Servicio 39
4.10.3 Características opcionales 40
4.11 Fin de la suscripción 40
4.12 Custodia y recuperación de claves 40
4.12.1 Política y prácticas de custodia y recuperación de claves 40
4.12.2 Políticas y prácticas de recuperación y encapsulación de claves de sesión 40

5 CONTROLES DE SEGURIDAD FÍSICA, DE GESTIÓN Y DE OPERACIONES 40
5.1 Controles físicos 41
5.1.1 Localización y construcción del sitio 41
5.1.2 Acceso físico 42
5.1.3 Energía y Aire acondicionado 43
5.1.4 Exposiciones al agua 44
5.1.5 Prevención y protección contra fuego 44
5.1.6 Almacenamiento de medios 44
5.1.7 Eliminación de residuos 44
5.1.8 Respaldo fuera de sitio 44
5.2 Controles procedimentales 45
5.2.1 Roles de confianza 45
5.2.2 Número de personas requeridas por tarea 45
5.2.3 Identificación y autenticación para cada rol 46
5.2.4 Roles que requieren separación de funciones 46
5.3 Controles de personal 46
5.3.1 Requerimientos de experiencia, capacidades y autorización 46
5.3.2 Procedimientos de verificación de antecedentes 47
5.3.3 Requerimientos de capacitación 47

5.3.4 Requerimientos y frecuencia de capacitación 47
5.3.5 Frecuencia y secuencia en la rotación de las funciones 48
5.3.6 Sanciones para acciones no autorizadas 48
5.3.7 Requisitos de contratación a terceros 48
5.3.8 Documentación suministrada al personal 49
5.4 Procedimiento de Registro de auditoría 49
5.4.1 Tipos de eventos registrados 49
5.4.2 Frecuencia de procesamiento del registro 50
5.4.3 Período de conservación del registro de auditoría 50
5.4.4 Protección del registro de auditoría 50
5.4.5 Procedimientos de respaldo de registro de auditoría 50
5.4.6 Sistema de recolección de información de auditoría (interno vs externo) 51
5.4.7 Notificación al sujeto que causa el evento 51
5.4.8 Evaluación de Vulnerabilidades 51
5.5 Archivos de registros 51
5.5.1 Tipos de registros archivados 51
5.5.2 Periodos de retención para archivos 52
5.5.3 Protección de archivos 52
5.5.4 Procedimientos de respaldo de archivo 52
5.5.5 Requerimientos para sellado de tiempo de registros 53
5.5.6 Sistema de recolección de archivo (interno o externo) 53
5.5.7 Procedimientos para obtener y verificar la información archivada 53
5.6 Cambio de clave 53
5.7 Recuperación de desastres y compromiso 55
5.7.1 Procedimiento para el manejo de incidente y compromiso 55
5.7.2 Corrupción de datos, software y/o recursos computacionales 56
5.7.3 Procedimientos de compromiso de clave privada de la entidad 56
5.7.4 Capacidad de continuidad del negocio después de un desastre 56
5.8 Terminación de una CA 56

6 CONTROLES TÉCNICOS DE SEGURIDAD 58
6.1 Generación e instalación del par de claves 59
6.1.1 Generación del par de claves 59
6.1.2 Entrega de la clave privada al suscriptor 60
6.1.3 Entrega de la Clave Pública al emisor del Certificado 60
6.1.4 Entrega de la clave pública de la CA a las partes que confían 60
6.1.5 Tamaño de la clave 60
6.1.6 Generación de parámetros de clave pública y verificación de calidad 61
6.1.7 Propósitos de usos de clave (Campo key usage x509 v3) 61
6.2 Controles de ingeniería del módulo criptográfico y protección de la clave privada 62
6.2.1 Estándares y controles del Módulo criptográfico 62
6.2.2 Control multi-persona de clave privada 63
6.2.3 Custodia de la clave privada 64
6.2.4 Respaldo de la clave privada 64
6.2.5 Archivado de la clave privada 64
6.2.6 Transferencia de clave privada hacia o desde un módulo criptográfico 65
6.2.7 Almacenamiento de la clave privada en el módulo criptográfico 65
6.2.8 Método de activación de clave privada 65
6.2.9 Métodos de desactivación de la clave privada 66
6.2.10 Destrucción de clave privada 67
6.2.11 Clasificación del Módulo criptográfico 67
6.3 Otros aspectos de gestión del par de claves 68
6.3.1 Archivo de la clave pública 68

6.3.2 Período operacional del certificado y período de uso del par de claves 68
6.4 Datos de activación 68
6.4.1 Generación e instalación de los datos de activación 68
6.4.2 Protección de los datos de activación 69
6.4.3 Otros aspectos de los datos de activación 69
6.5 Controles de seguridad del computador 69
6.5.1 Requerimientos técnicos de seguridad de computador específicos 70
6.5.2 Clasificación de la seguridad del computador 70
6.6 Controles técnicos del ciclo de vida 70
6.6.1 Controles para el desarrollo del sistema 71
6.6.2 Controles de gestión de seguridad 71
6.6.3 Controles de seguridad del ciclo de vida 71
6.7 Controles de seguridad de red 71
6.8 Sellado de tiempo (Time-stamping) 72

7 PERFILES DE CERTIFICADOS, CRL Y OCSP 72
7.1 Perfil del Certificado 72
7.1.1 Número (s) de versión 76
7.1.2 Extensiones del certificado 76
7.1.2.1 Key Usage 76
7.1.2.2 Extensión de política de certificados 76
7.1.2.3 Nombre alternativo del sujeto 76
7.1.2.4 Restricciones básicas 77
7.1.2.5 Uso extendido de la clave 77
7.1.2.6 Puntos de distribución de los CRL 77
7.1.2.7 Identificador de clave de Autoridad 78
7.1.2.8 Identificador de la clave del sujeto 78
7.1.2.9 QcStatements 78
7.1.3 Identificadores de objeto de algoritmos 78
7.1.4 Formas del nombre 78
7.1.5 Restricciones del nombre 79
7.1.6 Identificador de objeto de Política de Certificado 79
7.1.7 Uso de la extensión Restricciones de Política (Policy Constraints) 79
7.1.8 Semántica y sintaxis de los Calificadores de Política (Policy Qualifiers) 79
7.1.9 Semántica de procesamiento para la extensión de Políticas de Certificado (Certificate Policies) 79
7.2 Perfil de la CRL 79
7.2.1 Número (s) de versión 80
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
7.2.2.3 Puntos de distribución de las CRL 81
7.3 Perfil de OCSP 81
7.3.1 Número (s) de versión 81
7.3.2 Extensiones de OCSP 81

8. AUDITORIA DE CUMPLIMIENTO Y OTRAS EVALUACIONES 82
8.1 Frecuencia o circunstancias de evaluación 82
8.2 Identidad/calidades del evaluador 83
8.3 Relación del evaluador con la entidad evaluada 83
8.4 Aspectos cubiertos por la evaluación 83
8.5 Acciones tomadas como resultado de una deficiencia 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 85
9.1.4 Tarifas por otros servicios 85
9.1.5 Políticas de reembolso 85
9.2 Responsabilidad financiera 85
9.2.1 Cobertura de seguro 85
9.2.2 Otros activos 85
9.2.3 Cobertura de seguro o garantía para usuarios finales 85
9.3 Confidencialidad de la información comercial 86
9.3.1 Alcance de la información confidencial 86
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 87
9.4.4 Responsabilidad para proteger información privada 87
9.4.5 Notificación y consentimiento para usar información privada 87
9.4.6 Divulgación de acuerdo con un proceso judicial o administrativo 87
9.4.7 Otras circunstancias de divulgación de información 87
9.5 Derecho de Propiedad intelectual 87
9.6 Representaciones y garantías 88
9.6.1 Representaciones y garantías de la CA 88
9.6.2 Representaciones y garantías de la RA 88
9.6.3 Representaciones y garantías del suscriptor 88
9.6.4 Representaciones y garantías de las partes que confían 89
9.6.5 Representaciones y garantías de otros participantes 89
9.7 Exención de garantía 89
9.8 Limitaciones de responsabilidad legal 89
9.9 Indemnizaciones 89
9.10 Plazo y finalización 90
9.10.1 Plazo 90
9.10.2 Finalización 90
9.10.3 Efectos de la finalización y supervivencia 90
9.11 Notificación individual y comunicaciones con participantes 90
9.12 Enmiendas 91
9.12.1 Procedimientos para enmiendas 91
9.12.2 Procedimiento de publicación y notificación 91
9.12.3 Circunstancias en que los OID deben ser cambiados 91
9.13 Disposiciones para resolución de disputas 91
9.14 Normativa aplicable 91
9.15 Adecuación a la ley aplicable 92
9.16 Disposiciones varias 92
9.16.1 Acuerdo completo 92
9.16.2 Asignación 92
9.16.3 Divisibilidad 92
9.16.4 Aplicación (Honorarios de Abogados y renuncia de derechos) 92
9.16.5 Fuerza mayor 92
9.17 Otras disposiciones 92

10. DOCUMENTOS DE REFERENCIA 93

INTRODUCCIÓN

1.1 Descripción general

El Ministerio de Industria y Comercio (MIC), a través de la Subsecretaría de Estado de Comercio, se constituye en la Autoridad de Aplicación (AA) conforme lo dispone la Ley que rige la materia. La Dirección General de Firma Digital y Comercio Electrónico (DGFD&CE) es la dependencia designada para ejecutar las funciones atribuidas al MIC como AA.

Entre sus funciones principales se encuentran:

- Administrar la Autoridad Certificadora Raíz del Paraguay (CA Raíz)
- Dictar las normas que regulen el Servicio de Certificación Digital en el país
- Estudiar la Solicitud de Habilitación del Prestador de Servicios de Certificación (PSC) y emitir dictamen técnico-jurídico de aprobación o rechazo
- Auditar al PSC
- Evaluar la posible revocación de la Habilitación del PSC
- Imponer sanciones al PSC

La Habilitación del PSC, será aprobada por resolución ministerial, previo dictamen de la DGFD&CE, al igual que la revocación de su habilitación.

En la cúspide de la Jerarquía de la Infraestructura de Clave Pública del Paraguay (PKI Paraguay), por sus siglas en inglés Public Key Infrastructure se ubica la CA Raíz, la misma cuenta con un certificado auto firmado y aceptado por los terceros que confían en la PKI Paraguay.

Los certificados digitales emitidos por la CA Raíz y por el PSC se rigen y ajustan a la presente Política de Certificación (CP), cuyo cumplimiento es de carácter obligatorio.

La CP fue elaborada conforme a las recomendaciones establecidas en el RFC 3647

''INTERNET X.509 Public Key Infrastructure. Certificate Policy and Certification Practices Framework''; y contiene los principios y reglas relativos a la gestión de Certificados Digitales, las normas mínimas y básicas que debe cumplir el PSC, el uso de los certificados digitales, entre otras cuestiones relacionadas con la PKI Paraguay.

En resumen, esta CP es específicamente aplicable a:

- Autoridad Certificadora Raíz del Paraguay (CA Raíz)
- Prestador de Servicios de Certificación (PSC)
- Usuario Final
- Parte que confía

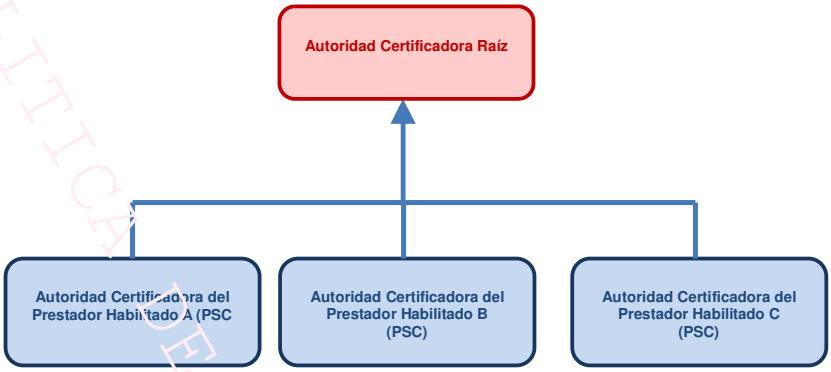
Esta política contempla los siguientes tipos de certificados:

- Certificado de CA Raíz
- Certificado de PSC
- Certificado de persona física para autenticación
- Certificado de persona física para firma digital
- Certificado de persona jurídica para autenticación
- Certificado de persona jurídica para firma digital

El PSC, una vez habilitado, pasa a ser parte de la cadena de confianza de la PKI Paraguay, y debe contar con un certificado digital firmado y emitido por la CA Raíz, generando de esta manera una estructura jerárquica como se muestra en la figura 1.

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.

Figura 1



1.2 Nombre e Identificación del documento

Nombre: Política de Certificación de la Infraestructura de Clave Pública del Paraguay

Versión: 3.0

Fecha de aprobación: 17 de diciembre de 2013

Sitio de internet oficial: www.acraiz.gov.py/documentación/politicas.pdf

1.3 Participantes de la PKI

1.3.1 Autoridades Certificadoras (CA)

Son las entidades autorizadas a emitir certificados de clave pública dentro de la PKI Paraguay. Esto incluye a:

- Autoridad Certificadora Raíz del Paraguay (CA Raíz)
- Prestador de Servicios de Certificación (PSC)

1.3.2. Autoridad de Registro (RA)

La RA ejecuta labores de identificación y autenticación de los solicitantes de un Certificado.

La misma, debe validar los requisitos de identificación del solicitante, dependiendo del tipo de Certificado y de la especificación de la Política pertinente. Además, tramita las Solicitudes de Revocacion de Certificados y valida la información contenida en las solicitudes de certificados.

La DGFD&CE y el PSC cumplen funciones de RA. El PSC podrá establecer sucursales en todo el territorio de la república respecto a las funciones de Registro bajo su responsabilidad, cumpliendo las normas y procedimientos establecidos en la normativa vigente, previa comunicación y autorización de la AA.

1.3.3. Suscriptores

Respecto a la CA Raíz, es suscriptor el PSC; en relación a este último, es suscriptor toda persona física o jurídica a quien se emite un certificado digital, dentro de la jerarquía PKI Paraguay.

1.3.4. Parte que confía

Es toda persona física o jurídica que confía en un certificado y/o en las firmas digitales generadas a partir de un certificado, emitidos dentro de la jerarquía PKI Paraguay.

Una parte que confía puede o no ser un suscriptor.

1.3.5. Otros participantes

Sin estipulaciones.

1.4 Uso del Certificado

1.4.1 Usos apropiados del Certificado

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 PSC.	Firma de certificado a sus suscriptores. Firma de CRL. • Firma de Certificado (Certificate Signing) • Firma de CRL (CRL Signing)
Certificado de persona física para firma digital	Firma digital • No repudio (Non-Repudiation)
Certificado de persona física para autenticación	Autenticación • Firma Digital (Digital Signature) • Cifrado de Clave (Key Encipherment)
Certificado de persona jurídica para firma digital	Firma digital • No Repudio (Non-Repudiation)
Certificado de persona jurídica para autenticación	Autenticación • Firma Digital (Digital Signature)

	• Cifrado de Clave (Key Encipherment) • Acuerdo de Clave (Key Agreement)

1.4.2. Usos prohibidos del certificado

Los certificados emitidos deben ser utilizados dentro del marco de la normativa vigente que rige la materia.

Cualquier otro uso de los certificados no especificado en esta CP y en la normativa vigente, está fuera del alcance y responsabilidad de esta CP. El uso indebido de los certificados será sancionado por la CA, pudiendo llegar a la revocación del mismo.

1.5 Administración de la Política

1.5.1. Organización que administra el documento

Nombre: Dirección General de Firma Digital y Comercio Electrónico (DGFD&CE).

Dirección: Avenida Mcal. López 3333. Asunción, Paraguay.

Teléfono: (+595) (21) 616-3000.

Dirección de correo electrónico: info-dgfdce@mic.gov.py.

Página Web: www.acraiz.gov.py.

1.5.2. Persona de Contacto

Nombre: Dirección General de Firma Digital y Comercio Electrónico (DGFD&CE).

Dirección: Avenida Mcal. López 3333. Asunción, Paraguay.

Teléfono: (+595) (21) 616-3000.

Dirección de correo electrónico: info-dgfdce@mic.gov.py.

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

El Director General de Firma Digital y Comercio Electrónico, será el encargado de determinar la adecuación de la Declaración de Prácticas de Certificación (CPS) de la PKI y de los PSC que deseen formar parte de la PKI Paraguay.

1.5.4 Procedimientos de aprobación de la Política de Certificación (CP)

El MIC aprobará el contenido de la presente Política de Certificación y sus posteriores enmiendas o modificaciones, por Resolución Ministerial. Se podrá someter a consulta en la que se invitará a entidades públicas y privadas para comentarios y sugerencias.

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.

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 de la Subsecretaría de Estado 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. 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 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.

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 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 Privada: Es una de las claves de un sistema de criptografía asimétrico que se emplea para generar una firma digital sobre un mensaje de datos y es mantenida en reserva por el titular de la firma digital.

Clave Pública: Es la otra clave del sistema de criptografía asimétrica, que es usada por el destinatario de un mensaje de datos para verificar la firma digital puesta en dicho mensaje. La clave pública puede ser conocida por cualquier persona.

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

Datos de activación: Valores de los datos, distintos 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, validación y firma de los Certificados; el proceso de generación es una función de la Autoridad de Registro, la validación y firma, 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.

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 documentos electrónico no ha sido alterado desde la transmisión por el iniciador hasta su recepción por el destinatario.

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 almacena 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 criptosistema 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#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 que confía en un certificado y/o en las firmas digitales generadas a partir de un certificado, emitidos bajo 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 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.

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

Acrónimo	Descripción
C	País (del inglés, Country)
CA	Autoridad Certificadora (CA por sus siglas en inglés Certificate Authority)
CA Raíz	Autoridad Certificadora Raíz del Paraguay
CI	Cédula de identidad
CIE	Cédula de identidad extranjera
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)
DGFD&CE	Dirección General de Firma Digital y Comercio Electrónico dependiente de la Subsecretaría de Estado de Comercio.
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).

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)
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)
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)
URL	Localizador uniforme de recursos (URL por sus siglas en inglés Uniform Resource Locator).

2 RESPONSABILIDADES DE PUBLICACION Y DEL REPOSITORIO

2.1. Repositorios

La CA Raíz y el PSC, son responsables de las funciones de Repositorio para su propia CA. Los mismos, deben publicar la Lista de Certificados Revocados de sus suscriptores.

2.2 Publicación de Información de Certificación

El PSC, debe mantener un repositorio en su sitio principal de internet que permita a las partes que confían verificar en línea la revocación de un Certificado y cualquier otra información necesaria para validar el estado del mismo.

El PSC, debe mantener publicada, entre otros aspectos la versión actualizada de:

- CP y CPS que implementan
- El Certificado de la CA Raíz
- La Lista de Certificados Revocados
- Proforma de contrato de Suscriptor
- Las Resoluciones que Habilitan, Suspenden o Revocan al PSC
- La información relevante de la última auditoría que hubiere sido objeto
- Leyes, decretos, reglamentos y resoluciones que rigen la actividad de la PKI Paraguay
- Identificación, domicilio y medios de contacto

La CA Raíz dispone del siguiente sitio de internet como repositorio público de información: http://www.acraiz.gov.py y cuyo acceso será irrestricto.

2.3 Tiempo o frecuencia de Publicación

Las enmiendas o modificaciones de la CP se publicarán de acuerdo con lo establecido en el punto 9.12 de esta Política.

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 esta Política

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

2.4 Controles de Acceso a los Repositorios

La información publicada en el Repositorio, es información accesible únicamente para consulta. Los PSC, deben establecer controles para prevenir que personas no autorizadas agreguen, eliminen o modifiquen información de su repositorio.

3 IDENTIFICACION Y AUTENTICACION

3.1 Nombres

3.1.1 Tipos de Nombres

En la sección 3.1.4 se explican las reglas para interpretación del código de identificación. El uso del campo número de serie (serial number OID 2.5.4.5) se establece como un Campo del nombre distintivo del sujeto. En concordancia a lo definido en la familia de estándares X.501

A continuación se presentan los formatos de los nombres para el suscriptor del certificado dependiendo de su tipo.

En el caso de la CA Raíz:

Campo	Ejemplo	Descripción
Country (C)	PY	Código de país es asignado de acuerdo al estándar ISO 3166
Organization (O)	Ministerio de Industria y Comercio	Ministerio de Industria y Comercio es el responsable la administración de la CA Raíz de Paraguay
Organization Unit (OU)	DGFD&CE	DGFD&CE dependiente de la Subsecretaría de Estado de Comercio
Common Name (CN)	Autoridad Certificadora Raíz del Paraguay	Nombre de la AC Raíz de la PKI Paraguay
Serial Number	RUC – 80009022 -5	RUC Número de Cédula Tributaria correspondiente al MIC.

En el caso del PSC

Campo	Ejemplo	Descripción
Country (C)	PY	Código de país es asignado de
Organization (O)	Firma Fiel SA	Denominación o Razón Social de la Persona Jurídica habilitada como PSC
Common Name (CN)	CA – Firma Fiel SA	CA + Nombre de la CA

Serial Number {OID: 2.5.4.5}	RUC 99999999-9	RUC Número de Cédula Tributaria correspondiente al PSC. Debe ser validada durante el proceso de registro.

En el caso del Suscriptor Persona Física

Campo	Ejemplo	Descripción
Country (C)	PY	El código de país es asignado de acuerdo al ISO 3166
Organization (O)	LUCAS ALCARAZ RIOS	Nombre del suscriptor, según documento de identificación, en mayúsculas y sin tildes.
Organization Unit (OU)	PERSONA FISICA	La Política identifica si se trata de un certificado para: Persona física o Persona jurídica.
Common Name (CN)	LUCAS ALCARAZ RIOS (FIRMA)	Nombre del suscriptor, según documento de identificación, en mayúsculas y sin tildes. El propósito debe ser FIRMA o AUTENTICACION
Serial Number {OID: 2.5.4.5}	CI 2304045	CI más Número de Cédula de Identidad para paraguayos o CIE más Cédula de identidad para extranjeros
Surname (SN) {OID: 2.5.4.4}	ALCARAZ RIOS	Se registran los dos apellidos del suscriptor, en mayúsculas y sin tildes.

GivenName (G) {OID:2.5.4.42}	LUCAS	Se registra el nombre de suscriptor, en mayúsculas y sin tildes

En el caso del Suscriptor Persona Jurídica

Campo	Ejemplo	Descripción
Country (C)	PY	Código de país es asignado de acuerdo al ISO 3166
Organization (O)	ARANDU S.A	Razón Social de la entidad, según inscripción en el Registro Público, en mayúsculas y sin tildes.
Organization Unit (OU)	PERSONA JURIDICA	Identifica si se trata de un certificado para: Persona física o Persona jurídica
Common Name	ARANDU SA (FIRMA)	Nombre del Suscriptor en mayúsculas y sin tildes o nombres de dominio de la organización. El propósito debe ser FIRMA o AUTENTICACION
Serial Number {OID: 2.5.4.5}	RUC 99999999-9	RUC Número de Cédula Tributaria correspondiente al suscriptor Debe ser validada durante el proceso de registro.

Subject alternative name	DNS=www.arandu.com.py	Este es un valor opcional donde pueden colocarse otros nombres de dominio, direcciones de correo electrónico, direcciones IP, u otros identificadores únicos. Este campo se aplica únicamente para los certificados de AUTENTICACION.

3.1.2. Necesidad de Nombres significativos

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

3.1.3. Anonimato o seudónimos de los suscriptores

A fin de dar cumplimiento efectivo al atributo de No Repudio característico de los Certificados de Firma Digital no se admite el anonimato. 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 PSC, Certificado de Persona Jurídica para firma digital y para autenticación

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 física para firma digital y para autenticación

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	CI 999999
Cédula de identidad para extranjero	CIE	CIE 999999

3.1.5 Unicidad de los nombres

La CA debe asegurar que el "nombre distintivo del suscriptor" *(subject distinguished name)* es único dentro de la PKI Paraguay.

3.1.6 Reconocimiento, autenticación y rol de las marcas registradas

Se prohíbe a los solicitantes de certificados de personas jurídicas que incluyan nombres en las solicitudes que puedan suponer infracción de derechos de terceros. En el caso de personas jurídicas, no se podrá volver a asignar un nombre de titular que ya haya sido asignado a un titular diferente.

La PKI Paraguay no arbitrará, mediará o resolverá ninguna disputa concerniente a la propiedad de nombres de dominio, nombres de empresas o instituciones y marcas registradas**.** La CA tiene el derecho de rechazar una solicitud de certificado a causa de conflicto de nombre.

3.2 Validación inicial de identidad

El proceso de comprobación de identidad de la persona física o jurídica cuyos datos se incluyen en un certificado digital tiene como objetivo garantizar que el suscriptor sea la persona identificada en la solicitud del certificado, y que la información que se incluya en el certificado sea exacta. En principio, la exactitud y veracidad de la información proporcionada

por el suscriptor es atribuida al mismo, sin perjuicio de la respectiva comprobación por parte de la CA.

3.2.1 Método para probar posesión de la clave privada

El solicitante del certificado debe demostrar que posee la clave privada correspondiente a la clave pública que deberá ser listada en el Certificado. La posesión de la clave privada, correspondiente a la clave pública para la que se solicita que se genere el certificado, quedará probada mediante el envío de la solicitud de certificado (CSR) en formato PKCS#10 u otras demostraciones criptográficas equivalentes, aprobadas por la DGFD&CE., en la cual se incluirá la clave pública firmada mediante la clave privada asociada.

3.2.2 Autenticación de identidad de Persona Jurídica

La CA, en su función de Registro debe validar la identidad de la empresa o institución solicitante. Como mínimo, se debe recabar el nombre o razón social, el RUC y los datos del representante legal debidamente acreditado. Posteriormente, la CA debe comprobar la información suministrada por el solicitante contra los datos oficiales correspondientes.

En el Certificado de Personas Jurídicas para autenticación, si el solicitante requiere incluir uno o más nombres de Dominio en el campo ‘’Nombre alternativo del Sujeto’’ (Subject alternative name). El PSC, debe verificar la información de dominio suministrada por el solicitante, contra los datos oficiales correspondientes.

3.2.3 Autenticación de identidad de Persona Física

El Proceso de autenticación de la identidad del solicitante del Certificado debe ser en forma presencial, para el efecto, el PSC en su función de Registro debe verificar la validez y la vigencia de los documentos presentados. Posteriormente, éste debe comprobar la información suministrada por el solicitante contra los datos oficiales correspondientes.

3.2.4 Información del Suscriptor no verificada

No aplica.

3.2.5. Validación de la Autoridad (Capacidad de hecho)

El PSC, debe determinar si el solicitante se encuentra apto para solicitar un tipo de certificado específico. Además, debe validar que el solicitante no posee impedimentos legales.

En el caso de Certificados de Personas Físicas, debe validar:

- Nombre y documento de identidad
- Mayoría de edad.

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

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

El PSC, debe verificar la información suministrada por el solicitante contra los datos oficiales correspondientes.

3.2.6. 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.

3.3 Identificación y autenticación para solicitudes de re emisión de claves

3.3.1 Identificación y autenticación para re emisión de claves rutinaria

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

La solicitud de revocación, debe ser solicitada por el suscriptor del certificado, por una entidad autorizada para tales propósitos o un tercero.

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

- La recepción de un mensaje de datos firmado digitalmente por el suscriptor del certificado o una solicitud por escrito en papel firmado por el suscriptor del certificado.
- Presencialmente a través de los procesos de autenticación, de identidad (secciones 3.2.2. y 3.2.3.)
- Cualquier otro medio aprobado por la DGFD&CE 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 del Certificado

4.1.1 Quién puede presentar una solicitud de certificado

En la siguiente lista se detallan las personas que pueden presentar una solicitud de certificado:

- Para el caso de certificado de PSC, el representante legal o apoderado con poder suficiente.

- Para el caso de certificado de persona física, cualquier 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 apoderado con poder suficiente.

4.1.2 Proceso de Inscripción y responsabilidades

La DGFD&CE tiene la responsabilidad de:

- Ejecutar el proceso de registro y verificación de identidad del PSC
- Validar la información suministrada en la solicitud de certificado (CSR)
- Velar que el PSC cumpla con los requisitos establecidos en la normativa vigente que rige la materia
- Informar al PSC de sus deberes y responsabilidades por el uso del certificado
- Emitir y entregar el certificado de acuerdo con la información suministrada por el solicitante

El PSC 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

El solicitante tiene las siguientes responsabilidades dependiendo del tipo de certificado:

Certificado de PSC

- Presentar la solicitud de Habilitación ante la AA conforme a las disposiciones de la normativa vigente
- Generar el CSR conforme a lo estipulado en el apartado 3.2.1 de la presente política
- Firmar el Acuerdo de Suscriptores

Certificado de Persona Física para firma digital y para autenticación

- Presentar la solicitud del certificado y proveer información correcta y verdadera
- Presentar las documentaciones de su identificación válida y vigente
- La generación del CSR conforme a lo estipulado en el apartado 3.2.1. de la presente política.
- Firmar el Acuerdo de Suscriptores

Certificado de Persona Jurídica para firma digital y para autenticación

- Presentar la solicitud del certificado y proveer información correcta y verdadera
- Presentar documentos de identificación, de personería jurídica y documento que acredite la representación legal, válidos y vigentes
- En caso de requerir que uno o varios nombres de DNS (Domain Name Server), formen parte del campo nombre alternativo del sujeto es necesario que el representante legal presente evidencia que el nombre de dominio solicitado está registrado a nombre de la organización que representa.
- La generación del CSR conforme a lo estipulado en el apartado 3.2.1. de la presente política
- Firmar el Acuerdo de Suscriptores

4.2. Procesamiento de la Solicitud del Certificado

4.2.1 Ejecución de las funciones de Identificación y Autenticación

Certificado de PSC

La encargada de estas funciones es la DGFD&CE, entidad que debe velar por la identificación y autenticación de acuerdo con las disposiciones establecidas en el punto 3.2

Certificado de Persona Física o de Persona Jurídica

La encargada de estas funciones es el PSC, entidad que 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 certificado

Certificado de PSC

La DGFD&CE es la encargada de llevar adelante el estudio y análisis de la aceptación o rechazo de la solicitud de certificado, conforme a la normativa y a lo establecido en esta política. Este trámite será resuelto por resolución ministerial.

Certificado de Persona Física o Jurídica

El PSC, debe rechazar la solicitud de certificado en los casos que no se de cumplimiento a la normativa vigente y a lo establecido en esta política.

4.2.3. Tiempo para procesar solicitudes de Certificado

El tiempo de procesamiento del CSR (lapso de tiempo entre la solicitud emitida a la CA y la emisión del certificado del suscriptor) cualquiera sea el caso, será en el menor tiempo posible. El plazo será determinado en la CPS.

4.3 Emisión del Certificado

4.3.1 Acciones de la CA durante la emisión de los certificados

Una vez ejecutadas las labores de identificación y autenticación de los solicitantes, la CA debe verificar que el solicitante cumpla con los requisitos establecidos en esta política, con las normas técnicas y legislación vigente que rige la materia.

La emisión de un certificado implica, la realización de las siguientes acciones por parte de la CA:

- Asegurarse que la generación de un par de claves y un certificado se haya realizado de manera segura de acuerdo a la sección 3.2.1
- Asociación del par de claves que corresponde al certificado con un suscriptor, y que el par de claves se encuentre en su posesión
- Emisión del certificado digital para su uso operativo, de acuerdo con el Nombre Distintivo asociado con el suscriptor. La CA Raíz, debe asegurarse que el certificado emitido pueda ser instalado por el PSC en presencia del personal asignado por la CA Raíz. El certificado debe haber sido firmado previamente por la CA que lo emitió.

4.3.2 Notificación al suscriptor sobre la emisión del Certificado Digital

Luego de emitido el certificado digital la CA debe notificar al suscriptor la emisión del mismo.

Esta notificación no será requerida en el caso que el certificado digital sea emitido en la infraestructura tecnológica de la RA, en presencia del suscriptor en un dispositivo de seguridad criptográfico. De este modo el certificado digital y las claves se encuentren en posesión del suscriptor desde su emisión o generación.

En el caso en que la emisión no sea en forma presencial el PSC podrá notificar al suscriptor por medios electrónicos que se ha creado el certificado digital, que se encuentra disponible y

la forma de obtenerlo.

4.4. Aceptación del Certificado

4.4.1 Conducta constitutiva de aceptación de certificado

Certificado de PSC

Una vez emitido el certificado, el PSC, debe firmar el Acuerdo de Suscriptores. Posteriormente se procederá a la instalación del certificado emitido en la infraestructura del PSC.

Certificado de Persona física y Jurídica

Una vez emitido el certificado por el PSC, el Suscriptor debe firmar digitalmente el Acuerdo de Suscriptores, con lo que verificará que el certificado funciona correctamente.

4.4.2 Publicación del Certificado por la CA

La CA no debe publicar información de los certificados emitidos en los repositorios de acceso público.

4.4.3 Notificación de la emisión del certificado por la CA 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

El uso de la clave privada correspondiente a la clave pública, contenida en el certificado, solamente debe ser permitido una vez que el suscriptor haya aceptado el certificado emitido, dicho uso, debe realizarse conforme a la normativa vigente, lo estipulado en esta política y el acuerdo de suscriptores respectivo.

Los suscriptores deben proteger su clave privada del uso no autorizado y una vez expirado o revocado el certificado, su uso queda expresamente prohibido.

Notificar a la CA sin dilación indebida:

- La pérdida, robo o extravío del dispositivo criptográfico,
- El compromiso potencial de su clave privada,
- La pérdida de control sobre su clave privada, debido al compromiso de los datos de activación o por cualquier otra causa,
- Las inexactitudes o cambios en el contenido del certificado que conozca o pudiera contener el suscriptor.

Certificado de CA raíz

La Clave privada y el certificado de la Autoridad Certificadora Raíz del Paraguay podrá ser utilizado con el único propósito de:

- firmar los certificados de PCS; y,
- firmar las Listas de Certificados Revocados (CRL) correspondientes

Certificado de PSC

La Clave privada y el certificado del PSC podrá ser utilizado con el único propósito de:

- firmar los certificados personas físicas y jurídicas para firma digital y para autenticación; y,
- firmar las Listas de Certificados Revocados (CRL) correspondientes

Certificado de persona física para autenticación y firma digital

El uso de los certificados emitidos por el PSC, debe ser acorde a lo dispuesto en el punto 6.1.7 de la presente política

Certificado de persona jurídica para autenticación y firma digital

Los certificados de persona jurídica para firma digital serán usados de conformidad a lo establecido en la normativa vigente.

En el caso que el titular del certificado sea una persona jurídica, serán responsables por el uso sus representantes o personas designadas.

Cada persona jurídica deberá desarrollar y establecer los mecanismos de seguridad informática y de infraestructura física, así como los reglamentos, procedimientos o políticas que considere pertinentes para resguardar y delimitar el uso de dicho certificado en su organización.

El uso de los certificados emitidos por el PSC, debe ser acorde a lo dispuesto en el punto 6.1.7 de la presente política

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

La parte que confía debe aceptar las estipulaciones establecidas en la presente política, en todo lo que les resulte aplicable, como condición indispensable para confiar en el certificado.

Antes de cualquier acto de confianza la parte que confía debe evaluar en forma independiente:

- Que el certificado sea utilizado para un propósito apropiado, y que no esté prohibido o restringido por la presente política. Las CA no son responsables de esta tarea.
- El estado del certificado y el estado de todos los certificados de las CA en la cadena que emitieron los certificados.

4.6 Renovación del certificado

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

El PSC debe solicitar la emisión del nuevo certificado a la CA Raíz, con una antelación mínima de seis meses a la expiración del tiempo de uso del certificado que posee, conforme al punto 5.6 de la presente CP.

4.6.1 Circunstancias para renovación de certificado

No aplica.

4.6.2 Quién puede solicitar renovación

No aplica.

4.6.3 Procesamiento de solicitudes de renovación de certificado

No aplica.

4.6.4 Notificación al suscriptor sobre la emisión de un nuevo certificado

No aplica.

4.6.5 Conducta constitutiva de aceptación de un certificado renovado

No aplica.

4.6.6 Publicación por la CA del certificado renovado

No aplica.

4.6.7 Notificación por la CA de la emisión de un certificado a otras entidades

No aplica.

4.7 Re-emisión de claves de certificado

La re-emisión del certificado no está permitida por esta CP, cuando un certificado requiera ser re-emitido debe solicitarse un nuevo certificado, de acuerdo con la sección 4.1 de este CP.

4.7.1 Circunstancias para re-emisión de claves de certificado

No aplica.

4.7.2 Quien puede solicitar la certificación de una clave pública

No aplica.

4.7.3 Procesamiento de solicitudes de re-emisión de claves de certificado

No aplica.

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

No aplica.

4.7.5 Conducta constitutiva de aceptación de un certificado re-emitido

No aplica.

4.7.6 Publicación por la CA de los certificados re-emitidos

No aplica.

4.7.7 Notificación por la CA de la re-emisión de un certificado a otras entidades

No aplica.

4.8 Modificación de certificados

4.8.1 Circunstancias para modificación del certificado

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.

4.8.2 Quién puede solicitar modificación del certificado

No aplica.

4.8.3 Procesamiento de solicitudes de modificación del certificado

No aplica.

4.8.4 Notificación al suscriptor de la emisión de un nuevo certificado

No aplica.

4.8.5 Conducta constitutiva de aceptación del certificado modificado

No aplica.

4.8.6 Publicación por la CA de los Certificados modificados

No aplica.

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

No aplica.

4.9 Revocación y suspensión

4.9.1 Circunstancias para la revocación

Certificado de CA

- Cuando existan evidencias de que su clave privada se encuentra comprometida, o con riesgo cierto de estarlo
- Cuando la información incluida en el certificado es incorrecta o ha cambiado
- incumplimiento del acuerdo de suscriptor

- Insolvencia, quiebra o liquidación del PSC
- Cese de actividades.
- Si se comprueba la expedición de certificados falsos
- Incumplimiento grave de la CP y/o CPS aplicable
- Uso indebido del certificado digital
- Si se constata que los procedimientos de emisión de los certificados han dejado de ser seguros
- Otras causales especificadas en la normativa y reglamentación vigente

Certificado de Persona Física y Jurídica para firma digital y para autenticación

- Cuando existan evidencias de que su clave privada se encuentra comprometida, o con riesgo cierto de estarlo
- Cuando se compruebe que el suscriptor ha comprometido su confiabilidad, desatendiendo los lineamientos de seguridad establecidos, proporcionado información falsa al PSC u omitido otra información relevante
- Por fallecimiento, ausencia legalmente declarada, incapacidad total o parcial de la persona física
- Insolvencia, liquidación, quiebra de una persona jurídica
- Cuando finaliza el acuerdo de suscriptor con el PSC, por cumplirse la vigencia del mismo o por voluntad propia del suscriptor.
- Cuando la información incluida en el Certificado ha cambiado
- Incumplimiento grave de la CP y/o CPS aplicable
- Incumplimiento del acuerdo de suscriptor
- Otras causales especificadas en la normativa y reglamentación vigente

4.9.2 Quien puede solicitar Revocación

Los habilitados para realizar la solicitud de revocación son:

- La CA que emitió el certificado
- El suscriptor del Certificado puede solicitar la revocación de su certificado. Para el caso de persona jurídica el representante legal o apoderado con poderes suficientes de la institución titular del certificado.
- Autoridad Judicial Competente
- Además, cualquier persona puede solicitar la revocación de un certificado ante la CA correspondiente presentando evidencia contundente del uso indebido del certificado, compromiso de la clave, fallecimiento del titular u otro motivo de revocación establecido en la normativa vigente y esta CP.

4.9.3 Procedimiento para la solicitud de revocación

La CA debe evaluar la solicitud de revocación presentada y verificar que la solicitud de revocación ha sido presentada por el suscriptor del certificado, por una autoridad competente o un tercero de acuerdo con la sección 3.4.

La solicitud de Revocación contendrá las causales y motivos del pedido de revocación. La solicitud mencionada, podrá ser hecha a través de un mensaje de datos firmado digitalmente por el suscriptor del certificado o un tercero con una solicitud por escrito conforme al punto 4.9.2 de la CP.

El procedimiento de revocación de un certificado se inicia con la solicitud de revocación y termina con la emisión de una nueva Lista de Certificados Revocados (CRL). Este procedimiento será realizado por la CA, quien tiene funciones propias de una RA de conformidad al punto 1.3.2 de esta CP.

En los casos que la solicitud de revocación provenga de una Autoridad Judicial Competente, la CA deberá evaluar la solicitud. Antes de comenzar con el proceso de

revocación se deberá notificar al suscriptor lo cual no implicará aun la revocación efectiva del certificado.

Un certificado revocado será válido únicamente para la verificación de firmas generadas durante el periodo en que el referido certificado era válido.

4.9.4 Periodo de gracia para solicitud de revocación

No se estipulan periodo de gracia para revocación de certificados.

4.9.5 Tiempo dentro del cual la CA debe procesar la solicitud de revocación

El plazo máximo entre la recepción de la solicitud de revocación y la actualización de la Lista de Certificados Revocados (CRL), indicando los motivos de la revocación, es de veinticuatro (24) horas.

4.9.6 Requerimientos de verificación de revocación para las partes que confían

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

Para ello, las partes que confían pueden verificar el estado del certificado mediante el servicio de: OCSP o CRL más reciente, proveída por la CA.

4.9.7 Frecuencia de Emisión del CRL

CA Raíz

La Lista de Certificados Revocados deberá ser actualizada y publicada cuando ocurra al menos uno de los siguientes hechos:

- Cuando se produzca la revocación de un certificado digital emitido al PSC
- Tres meses después de la última emisión del CRL

PSC

La Lista de Certificado Revocados debe actualizarse y publicarse una vez a la semana o cuando surja la revocación del certificado de un suscriptor. La CRL, debe cumplir las provisiones establecidas en el estándar X.509. Además se deberá publicar los Delta-CRL cada veinticuatro horas.

Se debe garantizar la disponibilidad de las CRL con un mínimo de 99% anual y un tiempo programado de inactividad máximo de 0.5% anual.

4.9.8 Latencia máxima para CRLs

La CA debe publicar la CRL en el repositorio en un plazo no mayor a una hora posterior a su generación. Puede también establecerse Delta-CRL.

4.9.9 Disponibilidad de verificación de revocación/ estado en línea

Toda CA debe mantener disponible un repositorio con información del estado de los certificados emitidos, el cual puede ser accedido vía web. Adicionalmente, el PSC debe implementar el servicio de validación en línea OCSP.

4.9.10 Requerimientos para verificar la revocación en línea

La parte que confía debe verificar el estado de un certificado en el cual desea confiar, utilizando los mecanismos de verificación del estado de certificados establecidos en la sección anterior.

4.9.11 Otras formas de advertencias de revocación disponibles

Sin estipulaciones

4.9.12 Requerimientos especiales por compromiso de clave privada

El PSC, deberá notificar en un plazo de veinticuatro horas como máximo a la DGFD&CE respecto a circunstancias que produzcan el compromiso de sus claves o su imposibilidad de

uso.

En caso que la clave privada de una CA se vea comprometida, dicha entidad debe revocar de inmediato los certificados emitidos de acuerdo a la legislación vigente, comunicando dicha acción a todos los suscriptores y terceros que confían.

4.9.13 Circunstancias para suspensión

Según la normativa no se aplica la suspensión del Certificado.

4.9.14 Quien puede solicitar la suspensión

No aplica.

4.9.15 Procedimiento para la solicitud de suspensión

No aplica.

4.9.16 Límites del período de suspensión

No aplica.

4.10 Servicios de comprobación de estado de Certificado

4.10.1 Características operacionales

El estado de los certificados debe estar disponible a través de los CRL publicados en un sitio principal de internet (en el URL especificado en el CP) y para los PSC, es obligatorio implementar un servicio OCSP.

4.10.2 Disponibilidad del Servicio

Los sistemas de distribución de CRLs y de consulta en línea del estado de los certificados deberán estar disponibles con un mínimo de 99% anual y un tiempo programado de inactividad máximo de 0.5% anual.

4.10.3 Características opcionales

Sin estipulaciones

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 establecidas en la presente política, antes del vencimiento (fecha de expiración).
- Expiración del certificado.

4.12 Custodia y recuperación de claves

4.12.1 Política y prácticas de custodia y recuperación de claves

La CA no debe custodiar claves de los suscriptores de ningún certificado, únicamente se mantienen respaldos de sus propias claves privadas de acuerdo con el Plan de Continuidad de Negocio.

Para los efectos del Plan de Continuidad de Negocio, las claves privadas de las CA deben estar en custodia y respaldadas bajo estrictas normas de seguridad, y almacenadas en dispositivos criptográficos FIPS 140-2 nivel 3, que garantizan la no divulgación de las claves.

4.12.2 Políticas y prácticas de recuperación y encapsulación de claves de sesión

No aplica

5 Controles de seguridad física, de gestión y de operaciones

La CA Raíz mantiene controles de seguridad no-técnicos (esto es, controles físicos, procedimientos y de personal) para asegurar la ejecución de las funciones de generación de clave, autenticación de los sujetos, emisión del certificado, revocación del certificado, auditoría y almacenamiento.

5.1 Controles físicos

5.1.1 Localización y construcción del sitio

La infraestructura tecnológica de la CA, necesariamente deberá situarse dentro del territorio paraguayo, por tanto no podrá utilizar una infraestructura tecnológica establecida en el extranjero.

Las operaciones de la CA, deben estar dentro de un ambiente de protección física que impida y prevenga usos o accesos no autorizados o divulgación de información sensible. Las instalaciones de la CA deben contar con al menos seis perímetros de seguridad física:

- Primer perímetro: acceso a las instalaciones de la CA (área de recepción)
- Segundo perímetro: acceso al área de procesos administrativos de la CA. Área interna al perímetro anterior, de acceso más estricto y restringido que el primero.
- Tercer perímetro: acceso al área de operación de la CA. Área interna al perímetro anterior, de acceso más estricto y restringido que el segundo.
- Cuarto perímetro: acceso al área de operaciones críticas de la CA. Área interna al perímetro anterior, de acceso más estricto y restringido que el tercero.
- Quinto perímetro: acceso al área de resguardo de documentos y dispositivos sensibles. Área interna al tercer perímetro
- Sexto perímetro: acceso al área de resguardo de clave privada. Área interna al cuarto perímetro

Las instalaciones donde se crean los certificados de la CA, se deben proteger con su propio y único perímetro físico, y las barreras físicas (paredes y barrotes) deben ser sólidas, extendiéndose desde el piso real al cielo raso real.

En el caso que en el periodo de operatividad del PSC, éste decida trasladar su infraestructura tecnológica principal y/o alterna a un sitio diferente del autorizado por la CA Raíz, se deberá cumplir cuanto sigue:

- Solicitar a la CA Raíz formalmente el traslado de su infraestructura tecnológica habilitada anteriormente, a un sitio que reúna las condiciones establecidas en la CP vigente
- La CA Raíz procederá a una inspección extraordinaria del nuevo sitio, a efectos de verificar el cumplimiento de los estándares de seguridad establecido en la CP vigente
- Aprobada la inspección, el PSC, procederá al traslado de la infraestructura tecnológica, conforme al procedimiento elaborado por él, con la conformidad de la CA Raíz. Si la inspección revelare, alguna anormalidad, el traslado será denegado, pudiendo el PSC solicitar una nueva inspección subsanada la irregularidad.
- La CA Raíz, designará personal técnico que intervendrá en el proceso de traslado, en especial de la clave privada.

5.1.2 Acceso físico

Los controles de acceso físico deben evitar el ingreso no autorizado a las instalaciones de la CA.

Para acceder al primer perímetro de seguridad se requerirá que todo individuo sea identificado por el personal autorizado. En este perímetro no se realizará ninguna operación ni proceso administrativo de la CA.

Para acceder al segundo perímetro de seguridad se requerirá un factor de autenticación y tarjeta de identificación visible. En este perímetro, se desarrollan procesos administrativos de la CA.

Para acceder al tercer perímetro de seguridad se requerirá 2 factores (contraseña y tarjeta de proximidad). Solo podrán acceder a él, personal autorizado por la CA. En caso que se autorice el acceso a terceros, estos deben ir acompañados por, al menos un personal de la CA. En ésta área se desarrollan actividades como: servicios de soporte, climatización, energía, comunicaciones, monitoreo, validación de CSR (Solicitud de firma de certificado), publicación en el repositorio, entre otras.

Para acceder al cuarto perímetro de seguridad se requerirá 2 factores de autenticación como mínimo (al menos uno de ellos debe ser biométrico). Solo podrán acceder a él, personal autorizado por la CA. En caso que se autorice el acceso a terceros, estos deben ir acompañados por al menos dos personales de la CA. En ésta área se realizan actividades de emisión y revocación de certificados, emisión de CRL.

El quinto perímetro de seguridad, constituye un recinto acorazado (cofre de seguridad), el acceso al mismo solo es permitido al personal autorizado. En ésta área se almacenan documentos y dispositivos sensibles inherentes a la operativa de la CA.

El sexto perímetro de seguridad, constituye un gabinete reforzado con cerraduras antirrobo (rack cofre), el acceso al mismo solo es permitido al personal autorizado. En ésta área se almacena la clave privada de la CA.

Cuando las instalaciones operacionales de la CA estén desocupadas, deben estar cerradas con clave y con las alarmas debidamente activadas.

Los perímetros deben ser auditados y controlados para verificar que solo puede tener acceso el personal autorizado debidamente identificado.

Los derechos de acceso a las instalaciones de la CA deben revisarse y actualizarse regularmente, al menos cada seis meses o cuando se presente movimiento del personal relacionado con labores de operación de la CA.

Los terceros que requieran acceso a las instalaciones operacionales de la CA, deben ser escoltados y registrarse ante el responsable de autorizar el acceso, la fecha y hora de entrada y salida.

5.1.3 Energía y Aire acondicionado

El equipo de la CA debe protegerse contra fallas en el fluido eléctrico corriente y otras anomalías en la energía, las instalaciones deben estar equipadas con sistemas de energía primario y de respaldo para asegurar continuidad del fluido eléctrico.

Las instalaciones deben contar con sistemas de aire acondicionado de precisión redundantes. El equipo instalado para climatizar el recinto, debe ser capaz de controlar la humedad relativa del mismo.

5.1.4 Exposiciones al agua

Las instalaciones de la CA deben ser construidas y equipadas para prevenir inundaciones y otros daños por exposición al agua, y deberán ser implementados procedimientos a tal efecto.

5.1.5 Prevención y protección contra fuego

Las instalaciones de la CA deberán ser construidas y equipadas para prevenir, detectar y suprimir incendios o daños producidos por la exposición a llamas o humo, y contar con procedimientos implementados para la prevención y protección al fuego.

5.1.6 Almacenamiento de medios

La CA debe asegurar el adecuado manejo y protección de los medios de almacenamiento de información, que contengan datos críticos o sensitivos del sistema, contra daños accidentales (agua, fuego, electromagnetismo) y debe impedir, detectar y prevenir su uso no autorizado, acceso o su divulgación.

5.1.7 Eliminación de residuos

La CA debe implementar controles para la eliminación de residuos (papel, medios, equipos y cualquier otro desecho) con el fin de prevenir el uso no autorizado, el acceso o divulgación de información privada y confidencial contenida en los desechos.

5.1.8 Respaldo fuera de sitio

La CA debe mantener respaldos de los datos críticos del sistema y de cualquier otra información sensible, incluyendo los datos de auditoría, en una instalación segura fuera del sitio principal.

Las copias de seguridad externas deben ser establecidas y mantenidas de conformidad con la política de continuidad del negocio y el plan de recuperación frente a desastres de manera compatible con los estándares internacionales.

5.2 Controles procedimentales

5.2.1 Roles de confianza

Las personas designadas para gestionar la infraestructura de la CA deben asumir ''Roles de Confianza'' para la asignacion de los mismos, se deberá considerar la contraposición de intereses.

Los Roles deben contemplar, al menos las siguientes responsabilidades:

a. responsabilidad general de administrar la implementación de las prácticas de seguridad de la CA;

b. aprobación de la emisión y revocación de los certificados;

c. instalación, configuración y mantenimiento de los sistemas de la CA;

d. operación diaria de los sistemas de la CA, respaldo y recuperación de sistemas;

e. funciones de auditoria interna para ejecutar la inspección y mantenimiento de los registros del sistema de la CA y de los registros de auditoría;

f. funciones de gestión del ciclo de vida de claves criptográficas (ejemplo: custodios de componentes de claves);

g. desarrollo de sistemas de la CA.

5.2.2 Número de personas requeridas por tarea

La CA debe establecer, mantener y ejecutar procedimientos de control rigurosos para asegurar la segregación de funciones, basados en las responsabilidades del trabajo y la

cantidad de personas de confianza que ejecutan las tareas sensibles (como mínimo dos personas).

5.2.3 Identificación y autenticación para cada rol

La CA debe confirmar la identidad y autorización de todo el personal que intente iniciar labores de confianza. La autenticación de la identidad debe incluir la presencia física de la persona y una verificación por medio de documentos vigentes de identificación legalmente reconocidos.

5.2.4 Roles que requieren separación de funciones

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

- 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.
- La auditoría interna de la operación de la CA debe ser ejecutada por un rol particular.

5.3 Controles de personal

5.3.1 Requerimientos de experiencia, capacidades y autorización

Las CA deben suscribir un documento con las personas designadas para desempeñar roles de confianza en el que se establecerá las funciones, obligaciones, responsabilidades y sanciones. Las personas designadas, 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

La CA debe contar con procedimientos para verificar la experiencia y los antecedentes del personal propuesto para un rol de confianza. Algunos aspectos de la investigación de antecedentes incluyen:

- Confirmación de empleos anteriores.
- Verificación de referencias profesionales.
- Título académico obtenido.
- Verificación de antecedentes judiciales y policiales.

5.3.3 Requerimientos de capacitación

Todo el personal involucrado en las operaciones de la CA debe estar capacitado apropiadamente, en aspectos tales como:

- operación del software y hardware
- políticas y procedimientos organizacionales
- procedimientos de seguridad y operacionales
- normativa vigente que rige la materia

5.3.4 Requerimientos y frecuencia de capacitación

La CA debe capacitar al personal cuando se presenten cambios significativos en las operaciones de la CA, por ejemplo cuando se producen actualizaciones de hardware o software, cambios en los sistemas de seguridad, etc.

La CA debe proveer los programas de entrenamiento y actualización a su personal para asegurar que el personal mantiene el nivel requerido de eficiencia para ejecutar sus labores satisfactoriamente.

5.3.5 Frecuencia y secuencia en la rotación de las funciones

La CA debe efectuar una rotación de sus roles de confianza. La frecuencia de la rotación del personal debe ser al menos:

- una vez cada tres años, para el PSC.
- una vez cada cinco años, para la CA Raíz.

Antes de asumir las nuevas labores, el personal debe recibir una nueva capacitación que le permita asumir las tareas satisfactoriamente.

5.3.6 Sanciones para acciones no autorizadas

La CA debe aplicar sanciones administrativas y disciplinarias al personal que violente las normas de seguridad establecidas en esta CP o su CPS, de acuerdo a lo estipulado en el documento suscripto para los roles de confianza.

5.3.7 Requisitos de contratación a terceros

La CA puede contratar personal externo o consultores bajo las siguientes condiciones:

- existe un contrato con cláusulas propias de los roles de confianza y estipula sanciones para las acciones no autorizadas.
- no se posee personal disponible para llenar los roles de confianza.
- los mismos cumplen con los mismos requisitos del punto 5.3.1.
- una vez finalizado el servicio contratado se revocan los derechos de acceso.

5.3.8 Documentación suministrada al personal

La CA debe suministrar suficiente documentación al personal para que ejecute un rol, donde se definen los deberes y procedimientos para el correcto desempeño de su función.

5.4 Procedimiento de Registro de auditoría

La CA debe mantener controles para proveer una seguridad razonable de que:

- los eventos relacionados con el ambiente de operación de la CA, la gestión de las claves y los certificados, son registrados exacta y apropiadamente;
- se mantiene la confidencialidad y la integridad de los registros de auditoría vigentes y archivados;
- los registros de auditoría son archivados completa y confidencialmente;
- los registros de auditoría son revisados periódicamente por personal autorizado.

5.4.1 Tipos de eventos registrados

La CA debe registrar los tipos de eventos que se presentan en sus operaciones. La CA debe mantener los registros manuales o automáticos, indicando para cada evento la entidad que lo causa, la fecha y hora del mismo. La CA debe registrar los eventos relacionados con:

- la gestión del ciclo de vida de las claves de la CA,
- la gestión del ciclo de vida del dispositivo criptográfico;
- la gestión del ciclo de vida del sujeto de certificado;
- la información de solicitud de certificados;
- la gestión del ciclo de vida del certificado;
- los eventos sensibles de seguridad;

Los registros de auditoría no deben registrar las claves privadas de ninguna forma y los relojes del sistema de cómputo de la CA deben estar sincronizados con el horario oficial de la república del Paraguay para un registro exacto de los eventos.

5.4.2 Frecuencia de procesamiento del registro

El personal del PSC con el rol de auditor debe realizar al menos una vez al mes revisiones de los registros de auditoría, sin necesidad de previo aviso; mientras que la CA Raíz debe realizar al menos una revisión de los registros cada cuatro meses.

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.

El procesamiento del registro de auditoría consiste en una revisión de los registros y la documentación de los motivos para los eventos significativos, y todas las acciones deben 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 Período de conservación del registro de auditoría

Las CA deben archivar los registros de auditoría de acuerdo a la sección 5.5.2.

5.4.4 Protección del registro de auditoría

Los registros de auditoría archivados deben mantenerse de forma de prevenir su revelación, modificación, destrucción no autorizada o cualquier otra intromisión.

5.4.5 Procedimientos de respaldo de registro de auditoría

La CA debe mantener copias de respaldo de todos los registros auditados.

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 PKI Paraguay.

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

La CA debe obtener información oportuna sobre las vulnerabilidades técnicas de los sistemas de información en uso. Además, se debe evaluar el riesgo a que se expone la organización ante esas vulnerabilidades y se deben tomar medidas para reducir el impacto.

5.5 Archivos de registros

5.5.1 Tipos de registros archivados

La CA debe almacenar los registros para establecer la validez de una firma y de la operación propia de la infraestructura PKI. Se deben archivar los siguientes datos:

Durante el inicio de operaciones de la CA:

- La Ceremonia de Claves en el caso de la CA Raíz,
- La Habilitación en caso del PSC,
- el CP y el CPS;
- Cualquier acuerdo contractual para establecer los límites de la CA;
- La configuración del sistema que requiere la CA

Durante la operativa de la CA:

- 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;
- documentación de recepción de dispositivos de almacenamiento de claves;
- todos los certificados y CRL (información de revocación) tanto emitidos o publicados;
- registros de auditoría;
- otros datos o aplicaciones para verificar el contenido de los archivos;
- todos los trabajos comunicados o relacionados a políticas, otras CA y cumplimiento de auditoría.

5.5.2 Periodos de retención para archivos

Todos los archivos deben mantenerse por un periodo de al menos diez años. Además de mantener los controles para que los archivos puedan ser revisados durante el periodo de retención definido.

5.5.3 Protección de archivos

Los archivos no deben modificarse o eliminarse por alguna operación no autorizada de la CA. La, misma debe mantener la lista de personas autorizadas a mover los registros a otros medios.

Los medios de almacenamientos deben estar guardados en instalaciones seguras, los registros deben ser etiquetados con un nombre distintivo, la fecha y hora de almacenamiento y la clasificación del tipo de información.

5.5.4 Procedimientos de respaldo de archivo

La CA debe mantener procedimientos adecuados de respaldo de archivos (físicos y electrónicos), tanto en el sitio principal como en el alterno, que aseguren la disponibilidad de los mismos, de acuerdo a un análisis de riesgos determinado por los factores de operación de la CA.

5.5.5 Requerimientos para sellado de tiempo de registros

No aplica

5.5.6 Sistema de recolección de archivo (interno o externo)

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

5.5.7 Procedimientos para obtener y verificar la información archivada

Solamente el personal de confianza autorizado está habilitado para obtener acceso al archivo. La CA debe realizar pruebas de restauración de la información archivada al menos una vez al año. La integridad de la información debe ser verificada cuando es restaurada.

5.6 Cambio de clave

La CA 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	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 PSC	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 Raíz 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.

Los responsables de las CA tendrán la obligación de garantizar que el tiempo máximo de uso en años de los certificados de niveles inferiores se ajusta con el tiempo operacional de todos los niveles superiores.

5.7 Recuperación de desastres y compromiso

5.7.1 Procedimiento para el manejo de incidente y compromiso

La CA debe contar con políticas y procedimientos formales para el reporte y atención de incidentes.

Las personas designadas que ejecutan roles de confianza deben velar por la seguridad de las instalaciones y la CA debe mantener procedimientos para que los mismos reporten los incidentes.

La CA debe establecer un plan de contingencia, que permita el restablecimiento y la continuidad del negocio, y la recuperación frente a desastres. Este plan debe contemplar las acciones a realizar, los recursos a utilizar y el personal a emplear en el caso de producirse un acontecimiento intencionado o accidental que inutilice o degrade los recursos y los servicios de certificación. Dicho plan, debe asegurar que los aspectos básicos del negocio, tales como: servicios de validación o revocación, puedan ser reasumidos en el menor tiempo posible.

Si la CA no puede ser reestablecida dentro de una semana, entonces su clave se reportará como comprometida y todos sus certificados son revocados. En casos excepcionales, la DGFD&CE, puede otorgar extensiones para la CA.

5.7.2 Corrupción de datos, software y/o recursos computacionales

Posterior a una corrupción de recursos computacionales, software o datos, la CA afectada debe realizar, en forma oportuna, un reporte del incidente y una respuesta al evento.

5.7.3 Procedimientos de compromiso de clave privada de la entidad

El plan de continuidad del negocio de la CA debe considerar el compromiso o sospecha de su clave privada como desastre. En este caso, se prevé la revocación del certificado, la publicación y difusión inmediata.

5.7.4 Capacidad de continuidad del negocio después de un desastre

La CA debe contar con un proceso administrativo para desarrollar, probar, implementar y mantener sus planes de continuidad del negocio.

La CA debe desarrollar, probar, mantener e implementar un plan de recuperación de desastres destinado a mitigar los efectos de cualquier desastre natural o producido por el hombre. Los planes de recuperación de desastres se enfocan en la restauración de los servicios de sistemas de información y de las funciones esenciales del negocio.

El sitio alterno debe contar con protecciones de seguridad física equivalentes al sitio principal.

El sitio alterno, deben tener la capacidad de restaurar o recobrar operaciones esenciales dentro de las veinticuatro horas siguientes al desastre, mínimamente con soporte para las siguientes funciones: revocación de certificados y publicación de información de revocación.

5.8 Terminación de una CA

La terminación de una CA 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
- Que la CA Raíz finalice sus servicios.

CA Raíz

En la eventualidad de que la CA Raíz del Paraguay finalice sus servicios deberá:

- Publicar en su sitio principal de internet la fecha de suspensión de los servicios con al menos 90 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 de las operaciones
- Notificar al PSC por lo menos 60 días antes de la suspensión efectiva o cese de sus operaciones
- Proceder a la revocación de todos los certificados emitidos que se encuentren vigentes a la fecha de la terminación
- Proceder a la destrucción de la clave privada de la CA Raíz del Paraguay mediante un mecanismo que impida su reconstrucción.

Por tanto, finalizado el servicio de la CA RAÍZ, el PSC no podrá continuar utilizando el certificado emitido por ella y los terceros aceptantes no deberán confiar en él.

PSC

Si se hallare comprometida la clave privada del PSC 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 PSC 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 de las operaciones
- 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.

La DGFD&CE 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.

6 CONTROLES TÉCNICOS DE SEGURIDAD

Todos los controles serán aprobados por la DGFD&CE, antes de que se pongan en práctica. En esta sección se definen las medidas de seguridad tomadas por la CA para proteger sus claves criptográficas y los datos de activación. La gestión de las claves es un factor crítico que permite asegurar que todas las claves privadas estén protegidas y solamente pueden ser activadas por personal autorizado.

6.1 Generación e instalación del par de claves

La CA mantendrá controles para brindar seguridad razonable de que los pares de claves de la CA, se generan e instalan de acuerdo con el protocolo definido para la generación de claves.

6.1.1 Generación del par de claves

El proceso de generación de claves ejecutado por la CA previene la pérdida, divulgación, modificación o acceso no autorizado a las claves privadas que son generadas. Este requerimiento aplica para toda la jerarquía de PKI Paraguay.

Certificados de CA Raíz

El par de claves de la CA Raíz, debe generarse mediante un proceso seguro por medio del módulo criptográfico de hardware (HSM – Hardware Security Module), que cumple como mínimo el estándar Fips 140-2 nivel 3. Dicha generación se realiza en las instalaciones de la CA, siguiendo los procedimientos establecidos en el guión de la Ceremonia de constitución de la CA Raíz del Paraguay.

Certificados de PSC

Las claves deben generarse mediante un proceso seguro por medio del módulo criptográfico de hardware (HSM – Hardware Security Module), que cumple como mínimo el estándar Fips 140-2 nivel 3 y a un procedimiento establecido por el PSC, en su CP, CPS u otro documento, acorde con la "ceremonia de generación de claves" implementada por la CA Raíz. El PSC garantizará que la clave privada de firma nunca permanecerá fuera del módulo donde fue generada, a menos que se almacene en un mecanismo de recuperación de claves.

El proceso de generación de claves de PSC debe producir claves que:

a. sean apropiadas para la aplicación o propósito destinado y que sean proporcionales a los riesgos identificados;

b. usen un algoritmo establecidos en la sección 7.1.3;

c. tengan una longitud de clave que sea apropiada para el algoritmo y para el período de validez del certificado de la PSC, de acuerdo con la sección 6.1.5 de tamaños de clave;

d. tomen en cuenta los requisitos del tamaño de clave de la CA Raíz

Certificados de persona física para firma digital y para autenticación

La generación de las claves de los suscriptores requiere que los módulos de criptografía asociados cumplan al menos con el estándar Fips 140-2 nivel 2

Certificados de persona jurídica para firma digital y para autenticación

La generación de las claves de los suscriptores requiere que los módulos de criptografía asociados cumplan al menos con el estándar Fips 140-2 nivel 3

6.1.2 Entrega de la clave privada al suscriptor

Se debe generar y mantener la clave privada dentro de los límites del módulo criptográfico, es decir el módulo criptográfico debe generar la clave privada localmente.

6.1.3 Entrega de la Clave Pública al emisor del Certificado

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 distribución de la clave pública se realiza a través del certificado digital y del repositorio público respectivo.

6.1.5 Tamaño de la clave

El tamaño de las claves debe ser suficientemente largo para prevenir que otros puedan determinar la clave privada utilizando cripto-análisis durante el periodo de uso del par de claves.

Certificado de CA

El tamaño de las claves para las CA debe tener mínimo 4096 bits RSA.

Certificado de persona física y jurídica

El tamaño de las claves para el suscriptor debe ser de 2048 bits RSA. La longitud de la clave pública que será certificada por la CA, debe ser menor o igual al tamaño de la clave privada de firma de la CA.

6.1.6 Generación de parámetros de clave pública y verificación de calidad

La CA genera y verifica los parámetros de clave pública de acuerdo con el estándar FIPS 186-2 (Digital Signature Standard-DSS) que define el cripto-algoritmo utilizado en la generación.

6.1.7 Propósitos de usos de clave (Campo key usage x509 v3)

Certificado de CA raíz

La Clave privada de la CA Raíz del podrá ser utilizado con el único propósito de:

- firmar los certificados digitales de PSC y,
- firmar la CRL correspondiente

El valor del campo key usage para este certificado es: KeyCertsign=1; OfflineCRLSign=1.

Certificado de PSC

La Clave privada del PSC podrá ser utilizado con el único propósito de:

- firmar los certificados de sus Suscriptores; y,
- firmar la CRL correspondiente

El valor del campo key usage para este certificado es: KeyCertsign=1; CRLSign=1.

Certificado de persona física para firma digital

El valor del campo key usage para este certificado es: nonRepudiaton=1.

Certificado de persona física para autenticación

El valor del campo key usage para este certificado es: digitalSignature=1; KeyEncipherment=1.

Certificado de persona jurídica para firma digital

El valor del campo key usage para este certificado es: NonRepudiaton=1.

Certificado de persona jurídica para autenticación

El valor del campo key usage para este certificado es: DigitalSignature=1; KeyAgreement=1; KeyEnchipherment=1.

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

6.2.1 Estándares y controles del Módulo criptográfico

Certificado de CA

La CA debe mantener controles para asegurar que su clave privada permanezca confidencial, mantenga su integridad, y que el acceso al hardware criptográfico esté limitado a personas autorizadas.

La copia de respaldo de la clave privada de la CA debe realizarse conforme se especifica en el punto 6.2.4 de la presente CP.

El estándar de módulos criptográficos es el "Security Requirements for Cryptographics Modules" (actualmente FIPS140). Los módulos criptográficos para la CA debe certificarse como mínimo con el FIPS 140-2 nivel 3

Certificado de persona física para firma digital y autenticación

El suscriptor debe cumplir con los controles definidos en el acuerdo de suscriptor y utilizar módulos criptográficos basados como mínimo en el estándar FIPS 140-2 nivel 2

Certificado de persona jurídica para firma digital y para autenticación

El suscriptor debe cumplir con los controles definidos en el acuerdo de suscriptor y utilizar módulos criptográficos basados como mínimo en el estándar FIPS 140-2 nivel 3

6.2.2 Control multi-persona de clave privada

Certificado de CA

Para la activación de la clave privada de firma de la CA se debe utilizar controles de acceso de múltiples partes (es decir, "m" de "n") con un valor mínimo de 3 para "m".

Si las claves privadas de la CA son respaldadas, éstas deben ser respaldadas, guardadas y recuperadas por personal autorizado con roles de confianza, utilizando controles múltiples en un ambiente físicamente seguro. La cantidad de personal autorizado para llevar a cabo esta función debe mantenerse al mínimo.

Certificado de persona física para firma digital y para autenticación

Sin estipulaciones

Certificado de persona jurídica para firma digital y para autenticación

Para la activación de la clave privada de persona jurídica para firma digital y para autenticación se debe utilizar controles de acceso que resguarden la clave privada. Una vez activado el dispositivo de firma, se debe mantener resguardado físicamente y monitoreado, para evitar el uso inapropiado.

6.2.3 Custodia de la clave privada

La CA no podrá almacenar ni copiar las claves privadas de sus suscriptores, ni de los módulos hardware que los contienen.

6.2.4 Respaldo de la clave privada

Los respaldos de clave privada de la CA son únicamente para propósitos de recuperación en caso de una contingencia o desastre. Los planes de continuidad del negocio de la CA deben incluir procesos de recuperación de desastres para todos los componentes críticos del sistema de la CA, incluyendo el hardware, software y claves, en el caso de falla de uno o más de estos componentes.

La clave privada de la CA debe ser respaldada, guardada y recuperada por personal autorizado con roles de confianza, utilizando controles múltiples en un ambiente físicamente seguro.

La copia de respaldo de la clave privada de la CA debe estar sujeta al mismo o mayor nivel de controles de seguridad que la clave que actualmente está en uso. La recuperación de la clave de la CA debe llevarse a cabo de una forma tan segura como el proceso de respaldo

La clave privada de certificado de firma digital del suscriptor no es respaldada por ningún motivo en la CA, y éstas permanecen dentro de los límites de los dispositivos criptográficos donde fue generada.

6.2.5 Archivado de la clave privada

La CA no archiva la clave privada de ninguno de sus suscriptores. En el caso de la CA, ésta debe archivar su par de claves (pública y privada) en concordancia con las disposiciones de protección de claves definidas en esta CP.

6.2.6 Transferencia de clave privada hacia o desde un módulo criptográfico

La clave privada de la CA es generada por un módulo criptográfico seguro, en caso de transporte de clave debe almacenarse de manera cifrada en un dispositivo seguro. Cuando la copia de seguridad o restauración, requiera la transferencia de la clave privada de o hacia el módulo criptográfico, éste debe estar sujeto a los mismos controles empleados para la generación de la clave original.

6.2.7 Almacenamiento de la clave privada en el módulo criptográfico

Los dispositivos criptográficos utilizados para el almacenamiento del respaldo de la clave privada de la CA debe ser guardado de forma segura, en un sitio alterno, con los mismos niveles de seguridad que el sitio principal, para que sea recuperado en el caso de un desastre.

Las partes de la clave secreta o los componentes necesarios para usar y gestionar los dispositivos criptográficos de recuperación de desastres, deberían estar también guardados con seguridad en una ubicación fuera del sitio principal.

La clave privada de la CA debe ser almacenada y utilizada dentro de un dispositivo criptográfico de hardware seguro que cumpla como mínimo con el perfil de protección apropiado de los requisitos del estándar FIPS 140-2 nivel 3

6.2.8 Método de activación de clave privada

Certificado de CA

Los métodos de activación de clave de la CA están protegidos y para accederlos se deben contar con mecanismos de autenticación de al menos dos factores de seguridad. Los datos de activación deben estar distribuidos en roles de confianza que ejecutan diversas personas.

Certificado de persona física para firma digital y para autenticación

Los métodos de activación de claves para un usuario deben contar con al menos un factor de seguridad.

Certificados de persona jurídica para firma digital y para autenticación

Los métodos de activación de claves para un usuario deben contar con al menos un factor de seguridad.

6.2.9 Métodos de desactivación de la clave privada

Certificado de CA

Para la CA Raíz es obligatorio que los módulos criptográficos, los cuales han sido activados, no estén desatendidos o abiertos al acceso no autorizado. Después de usarlos, estos deben ser desactivados manualmente o por un tiempo de expiración por estado pasivo.

En el caso del PSC, los equipos se mantienen en línea, para dichos efectos una vez activados los dispositivos criptográficos, estos se deben mantener monitoreados y protegidos contra accesos no autorizados.

Cuando la clave privada de la CA fuera desactivada, por expiración o revocación, ésta debe ser eliminada del módulo criptográfico. Se debe asegurar que no se permita la recuperación de copias.

Certificado de persona física para firma digital y para autenticación

Sin estipulaciones

Certificado de persona jurídica para firma digital y para autenticación

Cuando los equipos que hospedan los certificados de persona jurídica se encuentran en línea, éstos se deben mantener monitoreados y protegidos contra accesos no autorizados.

Cuando la clave privada fuera desactivada, por expiración o revocación, ésta debe ser eliminada del módulo criptográfico. Se debe asegurar que no se permita la recuperación de copias.

6.2.10 Destrucción de clave privada

El procedimiento para la destrucción de las claves privadas debe incluir la autorización para destruirlas.

Certificado de CA

La CA, eliminará sus claves privadas y el respaldo de las mismas cuando hayan expirado o hayan sido revocadas.

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).

Certificado de persona física para firma digital y para autenticación

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

Certificado de persona jurídica para firma digital y para autenticación

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

6.2.11 Clasificación del Módulo criptográfico

Certificado de PSC

La capacidad del módulo criptográfico del PSC es expresada en cumplimiento como mínimo del estándar Fips 140-2, nivel 3.

Certificado de persona física para firma digital y para autenticación

El módulo criptográfico para los suscriptores de personas físicas debe cumplir como mínimo con el estándar Fips 140-2, nivel 2.

Certificados de persona jurídica para firma digital y para autenticación

El módulo criptográfico para los certificados de persona jurídica debe cumplir como mínimo con el estándar Fips 140-2, nivel 3.

6.3 Otros aspectos de gestión del par de claves

La CA debe establecer los medios necesarios para gestionar en forma segura las claves de los suscriptores durante el ciclo de vida de las mismas.

6.3.1 Archivo de la clave pública

La CA debe mantener controles para sus propias claves, de acuerdo a lo estipulado en la sección 5.5. Las claves archivadas de la CA deberían estar sujetas al mismo o mayor nivel de control de seguridad que las claves que están en uso actualmente.

6.3.2 Período operacional del certificado y período de uso del par de claves

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

6.4 Datos de activación

La CA mantiene estrictos controles en los datos de activación para operar los módulos criptográficos y que necesitan ser protegidos. (ejemplo un PIN, un código de acceso o "password", autenticación biométrica).

6.4.1 Generación e instalación de los datos de activación

Certificado de CA

Se debe contar con datos de activación de múltiples factores para protección de los accesos al uso de claves privadas y su activación requiere de un control de múltiples partes (es decir, "m" de "n") con un valor mínimo de tres para "m".

Certificados de persona física para firma digital y para autenticación

Se deben generar e instalar sus propios datos de activación para proteger y prevenir perdidas, robos, modificación, divulgación o uso no autorizado de sus claves privadas.

Certificados de persona jurídica para firma digital y para autenticación

Se debe contar con controles para protección de los accesos al uso de claves privadas. En particular, se requiere generar sus propios datos de activación para prevenir uso no autorizado de la clave privada.

6.4.2 Protección de los datos de activación

Los datos de activación deberían ser memorizados, sin mantener respaldo escrito. Si se escriben, estos deberían de estar almacenados en un nivel de seguridad semejante al de los módulos criptográficos para protegerlos, y en una localización diferente a la de los mismos.

6.4.3 Otros aspectos de los datos de activación

Los datos de activación de los módulos criptográficos de la CA Raíz deben ser cambiados al menos una vez cada año. Y en el caso del PSC la frecuencia debe ser al menos una vez cada seis meses.

6.5 Controles de seguridad del computador

El equipo de la CA debe usar sistemas operativos que:

- Requieran autenticación de factores (como mínimo dos) para poder ser accedidos
- Provean capacidad para mantener registros de seguridad con fines de auditoría

- Cumplan con requerimientos y controles de seguridad, estrictos, definidos en su CP y CPS.

Luego de que la plataforma donde opera el equipo de la CA ha sido aprobada, debe continuar operando bajo los mismos parámetros aprobados.

6.5.1 Requerimientos técnicos de seguridad de computador específicos

Los equipos donde operan los sistemas de la CA, que requieran acceso remoto deben poseer autenticación mutua y los sistemas operativos deberían estar configurados de acuerdo con los estándares del sistema operativo de la CA y ser revisados periódicamente.

Las actualizaciones y parches de los sistemas operativos deberían ser aplicados de manera oportuna y la utilización de programas utilitarios del sistema debería ser restringida al personal autorizado, y debe estar estrictamente controlado.

El PSC, podrá introducir cambios tecnológicos siempre que éstos cumplan con la CP y CPS vigentes y sean notificados y aprobados por la CA Raíz.

6.5.2 Clasificación de la seguridad del computador

Los sistemas sensibles de la CA requieren un ambiente informático dedicado y aislado, que implemente el concepto de sede computacional confiable con procesos de auditoría.

6.6 Controles técnicos del ciclo de vida

La CA debe mantener controles en los equipos de seguridad (hardware y software) requeridos para operar en una infraestructura PKI desde el momento de la compra hasta su instalación, de forma que reduzcan la probabilidad que cualquiera de sus componentes sea violentado.

Todo el hardware y software que ha sido identificado para operar las CA debe ser enviado y entregado con métodos que provean una adecuada cadena de custodia. Y además, las configuraciones deben ser verificadas en un ambiente de prueba antes de iniciar operaciones.

6.6.1 Controles para el desarrollo del sistema

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

Los Administradores de la CA son los responsables de garantizar que se cumplan los procedimientos de seguridad correctamente. Además de ejecutar revisiones periódicas para asegurar el cumplimiento de los estándares de implementación de seguridad.

6.6.3 Controles de seguridad del ciclo de vida

La CA debe incluir controles en la gestión de seguridad por medio de herramientas y procedimientos que verifiquen la adherencia a la configuración de seguridad de los sistemas operativos y redes.

6.7 Controles de seguridad de red

El equipo de la CA debe estar dentro de los límites de la red interna, operando bajo un nivel de seguridad de red crítico. La red de la CA debe estar protegida contra ataques. Los puertos y servicios que no se requieran deben estar apagados.

En el caso de la CA Raíz debe estar off-line y aislada de la red organizacional.

Los niveles críticos de seguridad de red, deben incluir:

- La encriptación de las conexiones involucradas con las operaciones de la CA.
- Los sitios Web están provistos de certificados SSL.
- La red está protegida por firewalls y sistemas de detección de intrusos.
- Los accesos externos a información de bases de datos de la CA están prohibidos.
- La CA debe controlar la ruta de acceso del usuario desde la Terminal hasta los servicios.
- Los componentes de la red local deben mantenerse en un ambiente físicamente seguro y sus configuraciones deben ser auditadas periódicamente.
- Los datos sensibles deben encriptarse cuando se intercambian sobre redes públicas o no confiables.

La CA debe definir los procedimientos de control del cambio para el hardware, los componentes de la red y los cambios de configuración del sistema.

6.8 Sellado de tiempo (Time-stamping)

No aplica

7 PERFILES DE CERTIFICADOS, CRL Y OCSP

Este capítulo especifica el formato de las CRL y OCSP, tales como información del perfil, versión y extensiones utilizadas. En el caso de la CA Raíz, los OCSP no son utilizados, debido a que son pocos los certificados emitidos y por tanto revocados por ella. La verificación del estado de los certificados para el PSC constituye un factor crítico de seguridad para diversas aplicaciones, por lo tanto deben obligatoriamente implementar los dos métodos de validación: OCSP y CRL.

7.1 Perfil del Certificado

El certificado digital debe cumplir con:

- ITU-T X.509 V.3 Information technology Open systems interconnection The Directory: Public-key and attribute certificate frameworks
- RFC 5280: Internet X.509 Public Key Infrastructure Certificate and CRL Profile.
- ETSI TS 101 862 V.1.3.3 Qualified Certificates Profile
- RFC 3739 "Internet X.509 Public Key Infrastructure-Qualified Certificates Profile
- ISO 3166-1 "Códigos para la representación de los nombres de los países y sus subdivisiones. Parte 1: Códigos de los países".
- RFC – 3279 '' Internet X.509 Public Key Infrastructure Algorithm Identifier''

Cómo mínimo el certificado contiene:

Campo	Valor o restricciones
Versión (Version)	Los certificados deben ser X.509 versión 3 (V3).
Número de serie (Serial number)	Valor único emitido dentro del ámbito de cada CA.
Algoritmo de firma (Signature algorithm)	El Algoritmo de firma debe ser como mínimo SHA 256 RSA.
Emisor (Issuer DN)	Nombre de la CA Ver sección 7.1.4.
Válido desde (Valid from)	Este Campo especifica la fecha y hora a partir de la cual el certificado es válido. Las fechas establecidas para el periodo de validez deben ser sincronizadas con respecto a la hora oficial de la república del Paraguay.
Válido hasta (Valid to)	Este Campo especifica la fecha y hora a partir de la cual el certificado deja de ser válido. Las

	fechas para la validez del certificado deben ser sincronizadas con el horario oficial de la república del Paraguay.
Sujeto (Suscriber DN)	Nombre del suscriptor. Ver sección 7.1.4.
Clave pública del sujeto (Subject Public Key)	Codificado de acuerdo con el RFC 5280. Con un largo de clave mínima de 2048 bits y algoritmo RSA.
Extensiones	
Identificador de clave de la entidad emisora (Authority Key Identifier)	Este campo es usado por los diversos software de validación para ayudar a identificar a la autoridad certificadora que emitió el certificado en la cadena de confianza. Referencia el campo "Subject Key Identifier" de la CA. En el caso de la CA Raíz, este campo no debe especificarse.
Identificador de la clave del titular (Subject Key Identifier)	Este Campo es usado por el software de validación para ayudar a identificar un certificado que contiene una determinada clave pública.
Política del certificado (Certificate Policies)	Describe las políticas aplicables al certificado y la dirección URL donde se encuentra disponible la

	CP respectiva.
Uso de la clave (Key usage)	Debe indicar los usos permitidos de la clave. Este campo debe ser marcado como un CAMPO CRÍTICO. Ver sección 1.4.1 Usos apropiados del certificado
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, de tal forma que se pueda validar si el certificado en cuestión ha sido revocado o no.
Acceso a la información de la autoridad (Authority Information Access)	Este Campo es usado para indicar las direcciones donde puede ser encontrado el certificado de la CA. Además, para indicar la dirección donde puede accederse al servicio de OCSP, de tal forma que se pueda validar si el certificado en cuestión ha sido revocado o no. En el caso del certificado de la CA Raíz, este Campo no debe especificarse.
Usos extendidos de la clave	Referencia otros propósitos de la clave, adicionales al uso. De acuerdo con la sección 7.1.2.5. Solamente en el caso de certificado de persona física o jurídica este

	campo debe especificarse.
Restricciones básicas (Basic Contraitns)	Ver sección 7.1.2.4 Restricciones básicas.
Huella Digital (Thumbprint)	Resultado de aplicar algoritmos matemáticos a la información
QcStatements	Conforme al ETSI- TS 101 862 V.1.3.3.

7.1.1 Número (s) de versión

Todos los certificados emitidos dentro de la PKI Paraguay deben corresponder al estándar X.509 versión 3.

7.1.2 Extensiones del certificado

7.1.2.1 Key Usage

El "key usage" indica el uso del certificado de acuerdo con el RFC 5280 "Internet X.509 Public Key Infrastructure Certificate and CRL Profile". Ver sección 1.4.1 Usos apropiados del certificado. **Es una extensión crítica**

7.1.2.2 Extensión de política de certificados

En la extensión de "certificatepolicies" (Directivas del Certificado) debe detallar el nombre del dominio elegido por la CA y el directorio creado para el repositorio de dicho documentos. **Es una extensión crítica.**

7.1.2.3 Nombre alternativo del sujeto

La extensión "subjectAltName" es opcional y solamente se puede usar para certificados de agente de persona jurídica para autenticación. En caso de ser utilizada, el uso de esta extensión debe ser "no crítico" y únicamente está permitido el uso del nombre DNS, en concordancia con la sección 4.1.2.

7.1.2.4 Restricciones básicas

Para la CA, la extensión SubjectType (Tipo de asunto), debe tener el valor de ''CA''. En el caso de la CA Raíz la extensión PathLenConstraint (Restricción de longitud de ruta) debe tener el valor ''ninguno''; para el PSC, debe tener el valor ''cero'', para indicar que el mismo no permite más sub-niveles en la ruta del certificado y en el caso del certificado de persona física o jurídica, este campo no debe especificarse. **Es una extensión crítica**.

7.1.2.5 Uso extendido de la clave

La extensión permite configurar los propósitos de la clave. La extensión no es crítica. A continuación se presenta el cuadro con los propósitos comunes:

Descripción	Tipos de certificado
Autenticación del cliente	• De Persona Física para autenticación • De persona jurídica para autenticación
Autenticación de servidor	• De Persona Jurídica para autenticación
Protección del correo	• De persona física para firma digital
Smart Card Logon	• De persona física para autenticación

7.1.2.6 Puntos de distribución de los CRL

La extensión "CRL Distribution Points"(Puntos de Distribución) contiene las direcciones URL de la localización donde las partes que confían pueden obtener el CRL para verificar el estado del certificado. La extensión no es crítica.

7.1.2.7 Identificador de clave de Autoridad

El método para la generación del identificador está basado en la clave pública del PSC del certificado, de acuerdo a lo descrito por el RFC 5280 "Internet X.509 Public Key Infraestructura Certificate and CRL Profile". La extensión no es crítica.

7.1.2.8 Identificador de la clave del sujeto

El método para la generación del identificador de clave está basado en la clave pública del sujeto del certificado y es calculado de acuerdo con uno de los métodos descritos en el RFC 5280 "Internet X.509 Public Key Infrastructure Certificate and CRL Profile". La extensión no es crítica.

7.1.2.9 QcStatements

El "QcStatements" debe ser definido acorde al estándar ETSI-TS 101 862 V.1.3.3 "Qualified Certificate Profile". La extensión no es crítica

7.1.3 Identificadores de objeto de algoritmos

Los certificados generados dentro de la PKI Paraguay deben usar el siguiente algoritmo:

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 dentro de la PKI Paraguay deben cumplir las regulaciones de la sección 3.1.1. Adicionalmente, en el campo Suscriber DN (Sujeto) el certificado de suscriptor generalmente

debe incluir el URL donde se encuentra los términos del uso de los certificados y los acuerdos entre las partes.

7.1.5 Restricciones del nombre

Los nombres se escriben en mayúsculas y sin tildes, únicamente se debe aceptar el carácter ''Ñ ''como un caso especial para los nombres de personas físicas y jurídicas.

El código de país es de dos caracteres y se asigna de acuerdo al estándar ISO 3166-1 "Códigos para la representación de los nombres de los países y sus subdivisiones. Parte 1: Códigos de los países".

7.1.6 Identificador de objeto de Política de Certificado

La DGFD&CE gestionará la obtención del OID correspondiente a cada clase de certificado.

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

Sin estipulaciones.

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

El calificador de la política está incluido en la extensión de "certificate policies" y contiene una referencia al URL con la CP aplicable y a los acuerdos de partes que confían.

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

Sin estipulaciones.

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)	Ver sección 7.2.1
Algoritmo de firma (Signature Algorithm)	Algoritmo usado para la firma del CRL, puede ser como mínimo SHA256WithRSAEncryption
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
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 Paraguay soporta las CRLs X.509 versión 2.

7.2.2 CRL y extensiones de entradas de CRL

7.2.2.1 Número CRL (CRL Number)

Orden secuencial de emisión de CRL. Esta extensión es crítica

7.2.2.2 Identificador de clave de Autoridad

El método para la generación del identificador está basado en la clave pública del PSC del certificado, de acuerdo a lo descrito por el RFC 5280 "Internet X.509 Public Key Infraestructura Certificate and CRL Profile". La extensión no es crítica.

7.2.2.3 Puntos de distribución de las CRL

La extensión "CRL Distribution Points"(Puntos de Distribución) contiene las direcciones URL de la localización donde las partes que confían pueden obtener el CRL para verificar el estado del certificado. La extensión no es 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 se implemente debe cumplir lo estipulado en el RFC-2560 "X.509 Internet Public Key Infrastructure Online Certificate Status Protocol – OCSP".

7.3.1 Número (s) de versión

Debe cumplir al menos con la versión 1 del RFC2560 "X.509 Internet Public Key Infrastructure Online Certificate Status Protocol – OCSP".

7.3.2 Extensiones de OCSP

Sin estipulaciones.

8. AUDITORIA DE CUMPLIMIENTO Y OTRAS EVALUACIONES

De acuerdo al Art. 42 de la Ley Nro. 4017/2010 se 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.

La DGFD&CE o terceros designados por ella es responsable de ejecutar las auditorias, de acuerdo a lo estipulado en la normativa vigente.

Cada CA, debe implementar un programa de auditorías internas para la verificación de su sistema de gestión.

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

8.1 Frecuencia o circunstancias de evaluación

La Auditoría externa al PSC se debe ejecutar al menos una vez al año y los costos deben ser asumidos por el mismo.

De conformidad al Programa de auditoría interna cada CA, establecerá la frecuencia o circunstancias para su realización, pero en términos generales se espera que las mismas ejecuten al menos una auditoría al año.

8.2 Identidad/calidades del evaluador

El equipo de Auditoría (Interna o externa) debe estar conformado por personal calificado con experiencia en tecnología de la información, seguridad, tecnología de PKI y criptografía.

8.3 Relación del evaluador con la entidad evaluada

Para el caso de las Auditorías externas, los Auditores deben ser independientes e imparciales, quienes ejecutarán las evaluaciones acorde a los procedimientos establecidos.

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

Los elementos objeto de Auditoría son:

- Controles de seguridad física y estándares técnicos de seguridad
- Confidencialidad y calidad de los sistemas de control
- Integridad y disponibilidad de los datos
- Cumplimiento de los estándares tecnológicos
- Seguridad del Personal
- Cumplimiento de la Política y Declaración de Prácticas de Certificación
- Cumplimiento de la legislación vigente, entre otros.

8.5 Acciones tomadas como resultado de una deficiencia

La CA debe tener procedimientos para ejecutar acciones correctivas para las deficiencias detectadas tanto en las Auditorías externas como en las internas.

En caso de detectarse una irregularidad en la Auditoría externa realizada al PSC, 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 del PSC

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

La CA debe publicar en el sitio principal de internet los informes relevantes de las auditorías realizadas.

9. OTROS ASUNTOS LEGALES Y COMERCIALES

9.1 Tarifas

Este punto contiene las disposiciones aplicables acerca de los montos a ser percibidos por la CA.

9.1.1 Tarifas de emisión y administración de certificados

La tarifa por la emisión y administración de los certificados emitidos por una CA, estará determinada en la normativa vigente.

9.1.2 Tarifas de acceso a certificados

La CA, no se encuentra habilitada para el cobro de tarifas de acceso a certificados.

9.1.3 Tarifas de acceso a información del estado o revocación

La CA, no se encuentra habilitada para el cobro de tarifas de acceso a estado o revocación de los certificados.

9.1.4 Tarifas por otros servicios

La CA, no se encuentra habilitada para el cobro de tarifas para acceder a información de la Política y la Declaración de Prácticas de Certificación.

9.1.5 Políticas de reembolso

Para el caso del PSC, la política de reembolso debe estar establecida en su CP o CPS, y publicada en su sitio principal de internet.

9.2 Responsabilidad financiera

9.2.1 Cobertura de seguro

El PSC, debe contar 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

El PSC debe poseer suficientes recursos financieros para mantener sus operaciones y ejecutar sus deberes, asimismo debe ser razonablemente 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

En el caso que exista cobertura de seguro o garantía disponible para los suscriptores, el PSC debe establecer en su CPS los tipos correspondientes.

9.3 Confidencialidad de la información comercial

9.3.1 Alcance de la información confidencial

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

- 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

No será considerada información confidencial, la CRL ni la información del estado de los certificados.

9.4 Privacidad de información personal

9.4.1 Plan de Privacidad

La CA debe implementar 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 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 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

La CA, debe mantener en forma exclusiva todos los derechos de propiedad intelectual, con respecto a la presente documentación y aplicaciones pertenecientes a ella.

9.6 Representaciones y garantías

9.6.1 Representaciones y garantías de la CA

La CA debe garantizar que:

- No se presentan distorsiones en la información contenida en los certificados o en la emisión de los mismos.
- No existan errores en la información que fue introducida por la entidad que aprueba la emisión del certificado.
- Los certificados reúnen los requerimientos expuestos en esta CP.
- Los servicios de revocación y el uso de los repositorios cumplen lo estipulado en esta CP.

9.6.2 Representaciones y garantías de la RA

Las CA en su función de Registro debe asegurar que:

- No se presentan distorsiones en la información contenida en los certificados o en la emisión del mismo.
- No se presentan errores en la información del certificado que fue introducida por las entidades de registro.
- Que los dispositivos y materiales requeridos cumplen con lo dispuesto en esta CP.

9.6.3 Representaciones y garantías del suscriptor

El suscriptor debe garantizar que:

- Cada firma digital creada usando la clave privada corresponde a la clave pública listada en el certificado.

- La clave privada está protegida y que no autoriza a otras personas a tener acceso a la clave privada del suscriptor.
- Toda la información facilitada por el suscriptor y contenida en el certificado es verdadera.
- El certificado es utilizado exclusivamente para los propósitos autorizados.

9.6.4 Representaciones y garantías de las partes que confían

Las partes que confían requieren conocer suficiente información para tomar la decisión de aceptar el certificado.

9.6.5 Representaciones y garantías de otros participantes

Sin estipulaciones.

9.7 Exención de garantía

La CA debe establecer en su CP, CPS y otra documentación relevante, cualquier exención de responsabilidad que pudiera aplicárseles.

9.8 Limitaciones de responsabilidad legal

La CA debe establecer en su CP, CPS u otra documentación relevante cualquier limitación de responsabilidad que pudiera aplicársele, considerando las responsabilidades de privacidad, seguridad y diligencia en los procesos de certificación establecidas en este documento.

9.9 Indemnizaciones

La CA debe indemnizar a los suscriptores por cualquier causa legalmente establecida, se deberá demostrar ante las autoridades correspondientes los daños y perjuicios causados por ella.

9.10 Plazo y finalización

9.10.1 Plazo

La CP de la PKI empieza a ser efectiva una vez aprobado el contenido del documento por Resolución Ministerial y los nuevos certificados deben ser emitidos cumpliendo las políticas determinadas en la nueva versión de la CP.

La CP del PSC empieza a ser efectiva una vez publicada en su sitio de internet, previa aprobación del MIC, y los nuevos certificados deben ser emitidos cumpliendo las políticas determinadas en la nueva versión de la CP.

9.10.2 Finalización

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

9.10.3 Efectos de la finalización y supervivencia

La finalización de la vigencia de la CP, puede ser por derogación expresa, enmiendas o modificaciones; todos los certificados emitidos bajo esa política seguirán vigentes hasta que expiren o sean revocados, salvo que la nueva versión de la Política contemple aspectos críticos, en cuyo caso todos los certificados deberán ser revocados inmediatamente.

9.11 Notificación individual y comunicaciones con participantes

Toda comunicación entre la CA y el suscriptor, se realizará mediante mensaje de datos firmado digitalmente o documento escrito dirigido a cualquiera de las direcciones establecidas como contacto. Las comunicaciones electrónicas se harán efectivas una vez que la reciba el destinatario al que van dirigidas de igual manera en el caso de las escritas.

9.12 Enmiendas

9.12.1 Procedimientos para enmiendas

La DGFD&CE está facultada a introducir enmiendas o modificaciones, las que deberán ser documentadas y mantenerse a través de versiones y publicadas en el sitio de internet de la CA Raíz. Por resolución Ministerial, se fijará el plazo al cual, el PSC deberá ajustarse a la nueva versión.

Los cambios efectuados en la CP y CPS de los PSC deben ser revisados y aprobados por la DGFD&CE, antes de que éstos sean implementados. La documentación puede requerir una revisión.

9.12.2 Procedimiento de publicación y notificación

Toda enmienda o modificación de la CP, 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

En la eventualidad de cualquier disputa que implique los servicios o prestaciones que incluye la presente CP, CPS y normativa vigente, la parte afectada notificará primero a la CA y a todas las partes interesadas con relación a la disputa. La CA, asignará al personal adecuado para resolver el litigio extrajudicialmente.

9.14 Normativa aplicable

La CA estará sujeta a las leyes de la República del Paraguay, en particular a la normativa que rige la materia.

9.15 Adecuación a la ley aplicable

La presente Política de Certificación se adecua a legislación vigente aplicable a la materia.

9.16 Disposiciones varias

9.16.1 Acuerdo completo

No aplica

9.16.2 Asignación

No aplica

9.16.3 Divisibilidad

En el eventual caso que una cláusula de la política sea declarada 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)

No aplica

9.16.5 Fuerza mayor

Los Acuerdos de Suscriptores deben incluir cláusulas de fuerza mayor para proteger a la CA.

9.17 Otras disposiciones

El PSC habilitado de conformidad a los términos de la CP derogada, deberá adecuarse a las disposiciones de la presente CP en el plazo establecido por la Resolución que la ponga en vigencia.

La CP del PSC, debe guardar concordancia con las disposiciones de la presente Política.

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 de Costa Rica, Perú, Ecuador, Venezuela, Uruguay y Brasil.