DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN Y

POLÍTICA DE CERTIFICADOS

DE LA AUTORIDAD DE CERTIFICACIÓN RAÍZ DE VENEZUELA

CONTROL DE VERSIONES

VERSIÓN (EDICIÓN)	MOTIVO DEL CAMBIO	PUBLICACIÓN
1	Creación	Febrero 2007
2	Actualización General	Septiembre 2007
2.1	Actualización General	Abril 2008
2.2	Modificaciones en los campos: punto de distribución de CRL, acceso a la información de autoridad OCSP y Políticas del certificado.	Julio 2008
2.3	Actualización General	Septiembre 2010
3	Clasificación de la Norma	Enero 2011
3.1	Actualización General	Mayo 2011
3.2	Actualización General	Agosto 2011

ÍNDICE

<table>
<tr><th colspan="6">TRÁMITE</th></tr>
<tr><td colspan="6">1. DIRECTORIO</td></tr>
<tr><td colspan="2">NOMBRE</td><td colspan="4">CARGO SUSCERTE</td></tr>
<tr><td colspan="2"></td><td colspan="4">Superintendente
Directora de Registro y Acreditación
Directora de Inspección y Fiscalización
Director de Investigación y Desarrollo Tecnológico
Directora de la Oficina de Gestión Administrativa
Asesor Legal</td></tr>
<tr><td colspan="3">2. GRUPO DE TRABAJO: General</td><td colspan="3">3. COMISIÓN ESPECIAL:</td></tr>
<tr><td colspan="3">COORDINADOR:</td><td colspan="3"></td></tr>
<tr><td colspan="3">MIEMBROS PERMANENTES:</td><td colspan="3">CARGO:</td></tr>
<tr><td>NOMBRE</td><td>UNIDAD</td><td>CARGO</td><td colspan="3"></td></tr>
<tr><td></td><td></td><td></td><td colspan="3"></td></tr>
<tr><td rowspan="2"></td><td rowspan="2"></td><td rowspan="2"></td><td colspan="3">4. ESPECIALISTA(S) INVITADO(S):</td></tr>
<tr><td>NOMBRE</td><td>ENTIDAD</td><td>CARGO</td></tr>
<tr><td></td><td></td><td></td><td></td><td>SUSCERTE</td><td></td></tr>
<tr><td colspan="3">OBSERVACIONES</td><td colspan="3">RESPONSABLE DE LA EDICIÓN</td></tr>
<tr><td colspan="3" rowspan="3"></td><td colspan="3">COORDINADOR:

FECHA: FIRMA:</td></tr>
<tr><td colspan="3">SUPERINTENDENTE:

FECHA: FIRMA:</td></tr>
<tr><td colspan="3">APROBACIÓN APLICACIÓN EN:

FECHA: FIRMA:</td></tr>
</table>

1. OBJETO Y CAMPO DE APLICACIÓN

La Declaración de Prácticas de Certificación (DPC) de la Autoridad de Certificación (AC) Raíz de Venezuela, establece los elementos necesarios para la gestión de certificados a los Proveedores de Servicios de Certificación (PSC) del sector público y privado. La Política de Certificados (PC) con los tipos de certificados y el conjunto de reglas indican los procedimientos seguidos en la prestación de servicios de certificación creando la Infraestructura Nacional de Certificación Electrónica.

2. REFERENCIAS NORMATIVAS

2.1. Ley Orgánica de Procedimientos Administrativos (LOPA).

2.2. Decreto con Fuerza de Ley 1.204 Sobre Mensajes de Datos y Firmas Electrónicas (LSMDFE). (Febrero 2001)

2.3. Reglamento Parcial de la Ley Sobre Mensajes de Datos y Firmas Electrónicas. (Diciembre 2004)

2.4. Providencia administrativa de SUSCERTE Nº 016 Infraestructura Nacional de Certificación.

2.5. Norma SUSCERTE052, Plan de Continuidad del Negocio y Recuperación ante Desastres. Junio 2008.

2.6. RFC 2459 Internet X.509 Public Key Infrastructure Certificate and CRL Profile. 1999.

2.7. RFC 2560 Internet X.509 Public Key Infrastructure Online Certificate Status Protocol OCSP. 1999

2.8. RFC 3280 “Internet X.509 Public Key Infrastructure Certificate and Certificate. Revocation List (CRL) Profile”. Abril 2002.

2.9. RFC 3647 “Internet x.509 Public Key Infrastructure Certificate Policy and

Certification Practices Framework".

2.10. ETSI SR 002 176 Algorithms Parameters for secure electronics signature.

2.11. ETSI TS 101 456 "Policy requirements for certification authorities issuing qualified certificates", teniendo en cuenta los criterios de la CWA 14172-2 ("EESSI Conformity Assessment Guidance - Part 2: Certification Authority services and processes").

2.12. FIPS 140-2 Nivel 3. Security Requirements for Cryptographic Modules, (Diciembre 2002).

2.13. CWA 14172-2. EESSI Conformity Assessment Guidance – Part 2 – Certification Authority Services and processes 2004.

3. DEFINICIONES Y TERMINOLOGÍAS

A los efectos de esta guía se establecen las siguientes definiciones y terminologías:

ACREDITACIÓN	Título que otorga la Superintendencia de Servicios de Certificación Electrónica a los Proveedores de Servicios de Certificación (PSC) para proporcionar certificados electrónicos, una vez cumplidos los requisitos y condiciones establecidos en el Decreto-Ley 1.204.
AUDITOR REGISTRADO	Persona natural que actúa en forma propia o como representante de una persona jurídica que se encuentra registrado en SUSCERTE y avalado por esta para efectuar las evaluaciones y auditorías técnicas de los solicitantes y PSC.
CERTIFICADO ELECTRÓNICO	Mensaje de Datos proporcionado por un Proveedor de Servicios de Certificación que le atribuye certeza y validez a la Firma Electrónica.

DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN	Documento en el cual el Proveedor de Servicios de Certificación Electrónica, define los procedimientos relacionados con el manejo de los certificados electrónicos que emite.
POLÍTICA DE CERTIFICADOS	Documento en el cual el Proveedor de Servicios de Certificación Electrónica, define las reglas a seguir para el uso de un Certificado Electrónico en una comunidad de usuarios o aplicación determinados y sus requerimientos de seguridad.
ROOTVE	Aplicación desarrollada para crear y administrar certificados electrónicos X.509 de la Autoridad de Certificación Raíz.
REPOSITORIO	Sistema de información utilizado para el almacenamiento y acceso de los certificados electrónicos y la información asociada a los mismos.
SOLICITUD DE ACREDITACIÓN	Petición dirigida a SUSCERTE que tiene por objeto obtener la Acreditación para proporcionar certificados electrónicos y demás actividades previstas en el Decreto-Ley 1.204.
SUPERINTENDENCIA DE SERVICIOS DE CERTIFICACIÓN ELECTRÓNICA (SUSCERTE)	Servicio Autónomo que pertenece al Ministerio del Poder Popular para las Telecomunicaciones y la Informática cuyo objeto es acreditar, supervisar y controlar, en los términos previstos en el Decreto-Ley 1.204 (LSMDFE) y su Reglamento Parcial, a los Proveedores de Servicios de Certificación públicos o privados.
ITSEC	Recomendación europea de seguridad que establece criterios que permiten seleccionar funciones de seguridad arbitrarias (objetivos de seguridad que el sistema bajo estudio debe cumplir teniendo presentes las leyes y reglamentos).

4. SÍMBOLOS Y ABREVIATURAS

A los efectos de esta guía se establecen los siguientes símbolos y abreviaturas:

AAP	Autoridad de Aprobación de Políticas.
AC	Autoridad de Certificación.
AR	Autoridad de Registro.
DPC	Declaración de Prácticas de Certificación.
FUNDACITE	Fundación para el Desarrollo de la Ciencia y Tecnología.
HSM	Módulo de Hardware Criptográfico.
ICP	Infraestructura de Clave Pública.
ITSEC	Information Technology Security Evaluation Criteria.
LOAP	Ley Orgánica de Administración Pública.
LOPA	Ley Orgánica de Procedimientos Administrativos.
LCR	Lista de Certificados Revocados.
LSMDFE	Ley Sobre Mensajes de Datos y Firmas Electrónicas.
MPPTI	Ministerio del Poder Popular para la Ciencia, Tecnología e Industrias Intermedias.
OCSP	Online Certificate Status Protocol (Protocolo de estado de certificados en línea).
PC	Política de Certificados.
PIN	Personal Identification Number (Número de Identificación Personal).
PSC	Proveedor de Servicios de Certificación.
RBV	República Bolivariana de Venezuela.
RFC	Request for Comments
RPLSMDFE	Reglamento Parcial de la Ley Sobre Mensajes de Datos y Firmas Electrónicas.
SUSCERTE	Superintendencia de Servicios de Certificación Electrónica.

5. PROCEDIMIENTO

5.1 Principio Básico

El presente documento se constituye de la Declaración de Prácticas de Certificación y Política de Certificados de la Autoridad de Certificación Raíz del país, el cual sigue la estructura establecida por el RFC 3647.

6. DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN Y POLÍTICA DE CERTIFICADOS DE LA AUTORIDAD DE CERTIFICACIÓN RAÍZ DE VENEZUELA

6.1 Presentación

La AC Raíz es la Autoridad de Certificación Raíz de la Infraestructura Nacional de Certificación Electrónica cuya función principal es emitir los certificados electrónicos a los PSC. Donde el certificado electrónico asocia la identidad de un sujeto (autoridad, individuo, dispositivo, etc.) con su correspondiente clave pública y uno o más atributos.

El caso específico de un certificado raíz, corresponde a un certificado que ninguna autoridad de confianza superior firma digitalmente como raíz, es decir posee un certificado autofirmado y es a partir de allí, donde comienza la cadena de confianza. Este proceso de autofirmado hace que los campos del certificado raíz cumplan con los estándares internacionales y aplicables que garantizan la interoperabilidad.

Entonces la AC Raíz dispone de un certificado autofirmado con su clave

privada, con el que firma los certificados de clave pública de los PSC, que a su vez emplean sus claves privadas, para firmar los certificados de las entidades finales, de modo que toda la jerarquía se encuentra cubierta por la confianza de la AC Raíz.

La aplicación de la Infraestructura Nacional de Certificación Electrónica de la AC Raíz ha sido desarrollada por FUNDACITE Mérida organismo adscrito al Ministerio de Ciencia y Tecnología (MCT) en Software Libre siguiendo el Decreto Presidencial 3390.

El certificado electrónico es generado de acuerdo al estándar X.509 versión 3. El X.509 es el estándar fundamental que define la estructura del certificado de clave pública. Dicho estándar es generado por el sector de estandarización de Telecomunicación de la Unión Internacional de Telecomunicaciones (International Telecommunications Union-Telecommunications, ITU-T).

La arquitectura general, a nivel jerárquico de la Infraestructura Nacional de Certificación Electrónica se presenta en la figura Nº 1:

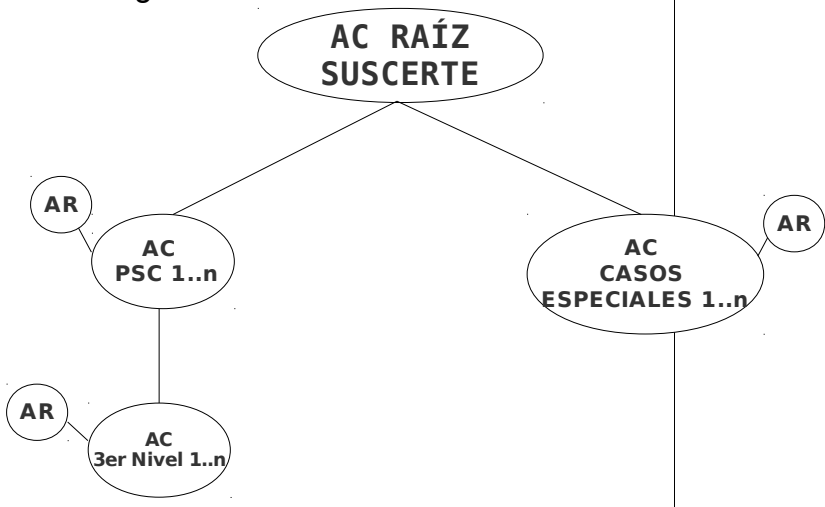

Figura Nº 1. *Arquitectura de la Infraestructura Nacional de Certificación Electrónica a nivel jerárquico*

La arquitectura jerárquica parte de la Raíz, ancla de la Cadena de Confianza de la certificación electrónica, llamada Autoridad de Certificación (AC) Raíz. Las relaciones de confianza se construyen desde la AC de más confianza hasta las que tenga la Infraestructura Nacional de Certificación Electrónica , donde no existe otra AC que pueda firmar el certificado de la AC Raíz. Este es el único caso, en el que la AC Raíz crea un certificado autofirmado por sí misma, para luego una vez acreditado ante SUSCERTE, según la Ley sobre Mensaje de Datos y Firma Electrónica (LSMDFE) firme el certificado electrónico de los PSC, además de la Lista de Certificados Revocados (LCR).

En el siguiente paso se encuentran las AC Subordinadas de la AC Raíz llamados PSC una vez acreditados ante SUSCERTE según la LSMDFE, y Casos Especiales, deben emitir los certificados según el propósito de los certificados electrónicos especificados en su propia DPC y PC.

En el tercer paso se encuentran las AC Subordinadas de tercer nivel, encargadas de proporcionar certificados electrónicos dentro de su ámbito o naturaleza de sus operaciones.

Es importante resaltar que SUSCERTE es responsable de elaborar y aprobar la presente DPC, así como sus modificaciones, siguiendo el modelo que la misma SUSCERTE proporciona para su elaboración. Si se considera necesario modificar la estructura entonces la elegida será el modelo a seguir por todos los que soliciten ser PSC acreditados y Casos Especiales. Además evalúa la DPC de cada PSC, Casos Especiales y AC de tercer nivel de la Infraestructura Nacional de Certificación Electrónica de Venezuela.

En consecuencia se debe tener en la DPC, las especificaciones de los requisitos empleados por la AC Raíz, para la generación, publicación y administración de certificados de firma electrónica a los PSC Subordinados y Casos Especiales, basado en el RFC 3647.

6.2 Nombre del Documento de Identificación

Nombre del documento	Declaración de Prácticas de Certificación (DPC) y Política de certificados (PC) de la AC Raíz
Versión del documento	3.1
Estado del documento	APROBADO
Referencia de la DPC/ OID (Object Identifier)	DPC/PC AC Raíz/OID 2.16.862.1.1
Fecha de emisión	Abril 2011
Fecha de expiración	La DPC y PC debe ser revisada con una periodicidad mínima de 2 años
Localización	Esta DPC y PC se encuentra en http://acraiz.suscerte.gob.ve

6.3 Comunidad de usuario y aplicabilidad

CAMPO DEL CERTIFICADO	Valor del Certificado Raíz
Versión	V3
Serial	Identificador único del certificado. Menor de 32 caracteres hexadecimales.
Algoritmo de firma	Debe contener el OID del algoritmo y de ser necesarios, los parámetros asociados usados por el certificador. Los algoritmos permitidos son SHA1, SHA256 y SHA384 with RSAEncryption.
DATOS DEL EMISOR (DN)	
CN	Autoridad de Certificacion Raiz del Estado Venezolano
O	Sistema Nacional de Certificacion Electronica

OU	Superintendencia de Servicios de Certificacion Electronica
C	VE (País)
E	acraiz@suscerte.gob.ve
L	(Dirección)
ST	(Estado)
PERÍODO DE VALIDEZ (VALIDITY)	
No antes de: (Not Before)	Fecha en que el período de validez del certificado comienza
No después de: (Not After)	Fecha en que el período de validez del certificado termina
DATOS DEL TITULAR	
CN	Autoridad de Certificacion Raiz del Estado Venezolano
O	Sistema Nacional de Certificacion Electronica
OU	Superintendencia de Servicios de Certificación Electronica
C	VE (País)
E	acraiz@suscerte.gob.ve
L	(Dirección)
ST	(Estado)
INFORMACIÓN DE LA CLAVE PÚBLICA (SUBJECT PUBLIC KEY INFO)	
Algoritmo de clave pública (Public Key Algorithm)	Algoritmo con el que se generó la Clave Pública (RSA) (RSAEncryption)
Tamaño de clave pública	4096 bits
EXTENSIONES	
Restricciones básicas (Basic Constraint)	Permite identificar si el signatario de un certificado es un certificador. Debe contener el atributo CA. CA: True y longitud del path = 2
Nombre alternativo del emisor (Issuer Alternative Name)	
DNSName	Nombre del DNS (suscerte.gob.ve)
OtherName Nº de Identif. OID 2.16.862.2.2	RIF-G-20004036-0
Identificador de clave del titular (Subject Key Identifier)	Medio para identificar certificados que contienen una clave pública particular, facilita la construcción de rutas de certificación (hash)
Identificador de clave de Autoridad Certificadora (Authority Key Identifier)	Medio para identificar la clave pública correspondiente a la clave privada utilizada para firmar un certificado
key id	Identificador de la clave

issuer	Contiene todos los datos del emisor
serial	Número serial
Uso de claves (Key usage)	Define el propósito de la clave del certif. Se debe definir como valor crítico: Firma electrónica del certificado y firma de LCR
Nombre alternativo del titular (Subject Alternative Name)	
DNSName	Nombre del DNS (suscerte.gob.ve)
Other Name	Other Name
Punto de distribución de LCR (CRL Distribution Point)	Indica como se obtiene la información de LCR URI:http://www.suscerte.gob.ve/lcr/ con LDAP URI:ldap://acraiz.suscerte.gob.ve/
Acceso a la Autoridad de Información (Authority Information Access)	OCSP, URI:http://ocsp.suscerte.gob.ve
Política de Certificados (Certificate Policies)	Incluye toda la información sobre la Política necesaria para la validación del certificado. (Lugar en internet desde donde se descargue la DPC y PC). URI:http://www.suscerte.gob.ve/dpc

Tabla Nº 1. *Estructura de los datos del certificado de la AC Raíz*

6.3.1 Autoridad de Registro (AR)

Las actividades de identificación y registro de los PSC deben ser realizados por SUSCERTE en conjunto con el proceso de acreditación, no existiendo autoridades de registro adicionales en el ámbito de la autoridad certificación raíz.

6.3.2 Titulares de Certificados

Los certificados emitidos por la AC Raíz tienen como titulares a la propia AC Raíz, a los PSC acreditados y Casos Especiales, según lo establecido en la LSMDFE y su Reglamento Parcial.

6.3.3 Proveedores de Servicios de Certificación, Casos Especiales

Las AC Subordinadas pueden ser PSC y Casos Especiales. En el marco legal venezolano, estos son derivados de la jerarquía de la AC Raíz, donde requieren que la AC Raíz les firme su certificado para que ellas a su vez emitan certificados a los signatarios finales siguiendo con la cadena de confianza desde el punto raíz de la Infraestructura Nacional de Certificación Electrónica . Cada una de estas AC subordinadas debe elaborar su propia DPC y Política de Certificados coherente con los requisitos generales establecidos por la LSMDFE, su Reglamento Parcial y otros que considere necesario SUSCERTE.

El Uso de Sha1withRSA se permite temporalmente por motivos de interoperabilidad con sistemas que no soportan Sha256 y SHA384 withRSA. Para Diciembre del año 2011 se debe revisar la DPC a fin de excluir Sha1withRSA.

La estructura de los datos del certificado electrónico para los PSC y Casos Especiales se presenta en la tabla Nº 2:

CAMPO DEL CERTIFICADO	Valor del Certificado de la AC principal del PSC
Versión	V3
Serial	Identificador único del certif. Menor de 32 caracteres hexadecimales.
Algoritmo de firma (Signature)	Debe contener el OID del algoritmo y de ser necesarios, los parámetros asociados usados por el certificador. Los algoritmos permitidos son SHA1, SHA256 y SHA384 withRSAEncryption.
DATOS DEL EMISOR	
CN	Autoridad de Certificacion Raiz del Estado Venezolano
O	Sistema Nacional de Certificacion Electronica
OU	Superintendencia de Servicios de Certificacion Electronica
C	VE (País)

E	Correo electrónico (acraiz@suscerte.gob.ve)
L	(Dirección)
ST	(Estado)
PERÍODO DE VALIDEZ (VALIDITY)	
No antes de: (Not Before)	Fecha en que el período de validez del certificado comienza
No después de: (Not After)	Fecha en que el período de validez del certificado termina
DATOS DEL TITULAR	
CN	Identificación del PSC y/o Casos Especiales
O	Sistema Nacional de Certificacion Electronica
OU	Nombre o razón social tal cual aparezca en el documento constitutivo
C	País
E	(correo electronico)
L	(Dirección)
ST	(Estado)
INFORMACIÓN DE LA CLAVE PÚBLICA (SUBJECT PUBLIC KEY INFO)	
Algoritmo de clave pública (Public Key Algorithm)	Algoritmo con el que se generó la Clave Pública (RSA)
Tamaño de clave pública	4096 bits
EXTENSIONES	
Restricciones básicas (Basic Constraint)	Permite identificar si el signatario de un certificado es un certificador. Debe contener el atributo CA. CA: True y longitud del path = 1
Nombre alternativo del emisor (Issuer Alternative Name)	
DNSName	Nombre del DNS (suscerte.gob.ve)
Other Name	Other Name
Nº de Identificación OID 2.16.862.2.2	RIF-G-20004036-0
Identificador de clave del titular (Subject Key Identifier)	Medio para identificar certificados que contienen una clave pública particular, facilita la construcción de rutas de certificación (hash)
Identificador de clave de Autoridad Certificadora (Authority Key Identifier).	Medio para identificar la clave pública correspondiente a la clave privada utilizada para firmar un certificado
key id	Identificador de la clave

issuer	Contiene todos los datos del emisor de certificado
serial	Número de serie del certificado
Uso de claves (Key usage)	Define el propósito de la clave del certificado. Debe especificar como valor crítico: Firma electrónica de certificados, Firma de LCR
Nombre alternativo del titular (Subject Alternative Name)	
DNS Name	(nombre de dominio del PSC y/o Casos Especiales registrado en nic.ve)
Other Name	Other Name
OID 2.16.862.2.1	(Código de identificación del PSC acreditado y/o Casos Especiales asignado por SUSCERTE)
OID 2.16.862.2.2	RIF-(RIF del PSC y/o Casos Especiales) de acuerdo al Anexo Nº 1 de esta norma
Punto de distribución de LCR (CRL Distribution Point)	Indica como se obtiene la información de LCR del PSC y/o Casos Especiales (lugar en internet desde donde se descargue la LCR)
Acceso a la Autoridad de Información (Authority Information Access)	(Enlace al servicio OCSP). Campo opcional
Política de Certificados (Certificate Policies)	Incluye toda la información sobre la Política necesaria para la validación del certificado. (Lugar en internet desde donde se descargue la DPC y PC).

Tabla Nº 2. *Estructura de los datos del certificado del PSC*

6.3.4 Terceros de buena fe

Son todas las personas que realicen transacciones utilizando certificados electrónicos provenientes de la Infraestructura Nacional de Certificación Electrónica y deciden aceptar y confiar en estos certificados.

6.4 Uso de los certificados

6.4.1 Usos permitidos para los certificados

El certificado electrónico raíz sólo puede utilizarse para la identificación de la propia AC Raíz y para la distribución de su clave privada de forma segura.

El uso de los certificados emitidos por la AC Raíz estará limitado a la firma de certificados electrónicos para autoridades subordinadas y la firma de las listas de certificados revocados (LCR) correspondientes.

6.4.2 Usos no permitidos para los certificados

El uso no permitido para los certificados emitidos por la AC Raíz son todos aquellos que no están explícitamente permitidos en el apartado anterior.

6.5 Políticas de Administración de la AC Raíz

6.5.1 Especificaciones de la Organización Administrativa

Nombre	Superintendencia de Servicios de Certificación Electrónica.
Correo electrónico	superintendencia@suscerte.gob.ve
Dirección	Av. Andres Bello. Torre BFC. Piso 13. Caracas Venezuela
Número de teléfono	(058-212) 578.5674
Número de Fax	(058-212) 572.4932
Sitio Web	http://www.suscerte.gob.ve

6.5.2 Persona Contacto

Nombre	Superintendencia de Servicios de Certificación Electrónica.
Correo electrónico	superintendencia@suscerte.gob.ve
Dirección	Av. Universidad, Esquina El Chorro. Torre MCT. Piso 8. Caracas Venezuela
Número de teléfono	(058-212) 578.5674
Número de Fax	(058-212) 572.4932
Sitio Web	http://www.suscerte.gob.ve

6.5.3 Competencia para determinar la adecuación de la DPC a las políticas

La AAP de la AC Raíz es la responsable de determinar la adecuación de la DPC a los estándares y mejores prácticas en la materia.

7. PUBLICACIÓN DE INFORMACIÓN DE LA AC RAÍZ Y REPOSITORIOS DE LOS CERTIFICADOS

7.1 Repositorios

Los Certificados de la AC Raíz deben estar disponibles los 365 días del año, durante las 24 horas del día, y en caso de interrupción por causa de fuerza mayor, el servicio se restablecerá en el menor tiempo posible.

- **Para los certificados de la AC Raíz, los PSC acreditados y/o**

Casos Especiales:

web: http://acraiz.suscerte.gob.ve/

Sección: Certificados

- **Para la lista de certificados revocados (LCR):**

  web: http://acraiz.suscerte.gob.ve/lcr

  Sección: Lista de Certificados Revocados

  LDAP: ldap://acraiz.suscerte.gob.ve

- **Para la DPC:**

  web: http://acraiz.suscerte.gob.ve/dpc

  Sección: Declaración de Prácticas de Certificación

- **Servicio de validación en línea que implementa el protocolo OCSP:**

  web: http://ocsp.suscerte.gob.ve/

El repositorio público de la AC Raíz no contiene ninguna información confidencial o privada.

7.2 Publicación

Es obligación para la AC Raíz, Casos Especiales y los PSC pertenecientes a la jerarquía de la Infraestructura Nacional de Certificación Electrónica publicar la información relativa a sus DPC, certificados y el estado actualizado de dichos certificados.

Las publicaciones que realice SUSCERTE, de toda información clasificada como pública, se anunciarán en su sitio Web de la siguiente manera:

- La Lista de Certificados Revocados (LCR), se encuentra disponible en formato LCR V2, en el repositorio de la AC Raíz.
- La Declaración de Prácticas de Certificación y Política de Certificados de la AC Raíz, se encuentra disponible en el sitio Web de la AC Raíz: http://acraiz.suscerte.gob.ve/dpc en formato PDF.
- Todas las versiones del presente documento son públicas y se encuentran disponibles en el sitio Web de la AC Raíz: http://acraiz.suscerte.gob.ve en formato PDF.
- El certificado de la AC Raíz se encuentra disponible en el repositorio público, en formato X.509 v3 y en la dirección http://acraiz.suscerte.gob.ve. Sección: certificados.
- Los certificados emitidos por la AC Raíz se encuentran disponibles en el repositorio público, en formato X.509 v3 y en la dirección http://acraiz.suscerte.gob.ve. Sección: certificados.
- Los datos de contacto de SUSCERTE se encuentran en la dirección http://www.suscerte.gob.ve/index.php/es/contactos

7.3 Frecuencia de Publicación

7.3.1 Certificados de la AC Raíz

La publicación del certificado electrónico se realizará con anterioridad a su puesta en vigencia a través de la Gaceta Oficial. El periodo de validez es de veinte años.

7.3.2 Certificados del PSC

La publicación del certificado se realizará con anterioridad a su puesta en vigencia a través de la Gaceta Oficial. El periodo de validez es de diez (10) años.

7.3.3 Lista de Certificados Revocados (LCR)

La LCR se encuentra en el repositorio público de SUSCERTE, esta lista es actualizada:

- **Periódicamente**:

  Cada 6 meses a menos que suceda una acreditación o una revocación de un certificado dentro de la Infraestructura Nacional de Certificación Electrónica . Cuando suceda uno de estos eventos, el período de 6 meses es reiniciado.

- **Eventualmente:**

  Cada vez que se acredite o revoque un certificado dentro de la Infraestructura Nacional de Certificación Electrónica .

  Cada vez que sea revocado un certificado electrónico emitido por la AC Raíz.

7.3.4 Declaración de Prácticas de Certificación

La AC Raíz, publica en el repositorio, las nuevas versiones de este Documento, en forma inmediata luego de su aprobación.

7.3.5 Casos Especiales

La publicación del certificado se realizará con anterioridad a su puesta en vigencia a través de la Gaceta Oficial. El periodo de validez es de quince (15) años.

7.4 Controles de Acceso al Repositorio de Certificados

El acceso a la información publicada por la AC Raíz solo será de consulta y no podrá ser modificada por personas no autorizadas. La información pública solo será actualizada por el personal encargado de esta función que labora en SUSCERTE. Además se garantiza la consulta a la LCR y DPC en sus versiones anteriores y actualizadas.

8. IDENTIFICACIÓN Y AUTENTICACIÓN

8.1 Registros de Nombres

8.1.1 Tipos de Nombres

La AC Raíz, sólo genera y firma certificados con tipos de nombres acordes al estándar X. 500.

Para el certificado de la AC Raíz: El titular (subject) y el emisor (issuer), está formado por los siguientes atributos:

- CN = Autoridad de Certificacion Raiz del Estado Venezolano
- O = Sistema Nacional de Certificacion Electronica
- OU = Superintendencia de Servicios de Certificación Electrónica
- C = VE
- E = acraiz@suscerte.gob.ve

El nombre alternativo de la AC Raíz está formado por los siguientes atributos:

- DNSName=suscerte.gob.ve
- OtherName=
- OID 2.16.862.2.2=RIF G-20004036-0

Para los Certificados de PSC y Casos Especiales: El titular (subject) de los certificados esta formado por los siguientes atributos:

- CN = Identificación del Proveedor de Servicios de Certificacion y/o Casos Especiales
- O = Sistema Nacional de Certificacion Electronica
- OU = [nombre o razón social]
- C = VE
- E =[correo electrónico de contacto]

El emisor (issuer) de los certificados de PSC y/o Casos Especiales esta formado por los siguientes atributos:

- DNSName=[nombre de dominio registrado en nic.ve]
- OtherName=
- OID 2.16.862.2.1=[Código de identificación asignado por SUSCERTE]

- OID 2.16.862.2.2=RIF

SUSCERTE establece en esta política la emisión de tres tipos de certificados. Cada tipo de certificado se identificará por un OID (Object Identifier) único, incluido en el certificado como identificador de política, dentro de la extensión X.509 Certificate Policies.

Certificado tipo I – Certificados para AC Raíz

(OID política 2.16.862.1.2)
Este certificado lo genera la Autoridad de Certificación para su identificación. Este es el certificado raíz autofirmado de primer nivel de la Infraestructura Nacional de Certificación Electrónica . El uso de este certificado está enmarcado en las actividades de la AC Raíz.

Certificado tipo II – Certificados de AC para PSC y Casos Especiales

(OID política 2.16.862.1.3)
Estos certificados se emitirán a los PSC acreditados ante SUSCERTE y Casos Especiales, según lo establecido en la LSMDFE y su reglamento parcial. Este tipo de certificado puede emitir otros certificados y tiene privilegio de AC Subordinada de la Infraestructura Nacional de Certificación Electrónica .

8.1.2 Necesidad de que los nombres sean significativos

SUSCERTE garantiza que los nombres distintivos (DN) de los certificados son suficientemente significativos para vincular la clave pública con una identidad.

8.1.3 Interpretación de formatos de nombres

Las reglas utilizadas para la interpretación de los nombres distinguidos en los certificados emitidos están descritas en la ITU-T X.500 Distinguished Name (DN). Adicionalmente todos los certificados emitidos utilizan codificación UTF8 para todos los atributos, según la RFC 3280

8.1.4 Unicidad de los nombres

La AC Raíz define el campo DN (Distinguished Name) del Certificado de Autoridad como único y sin ambigüedad. Para ello se incluirá como parte del DN, específicamente en el campo OU, el nombre o razón social del PSC y/o Casos Especiales. Por lo tanto, la unicidad se garantiza mediante la confianza sobre la unicidad de los nombres mercantiles en el registro mercantil nacional.

8.1.5 Resolución de conflictos relativos a nombres

SUSCERTE no actúa como árbitro o mediador, ni resuelve ninguna disputa relativa a la titularidad de nombres de personas u organizaciones, nombres de dominio, marcas o nombres comerciales, etc. Así mismo, este organismo se reserva el derecho de no aprobar una solicitud de certificado debido a conflicto de nombres.

8.2 Validación Inicial de la Identidad

8.2.1 Método de prueba de posesión de la clave privada

El sistema de certificación implementado y utilizado por SUSCERTE para la administración del ciclo de vida de sus certificados controla y garantiza de forma automática la emisión del certificado firmado al poseedor de la clave privada correspondiente a la clave pública incluida en la solicitud. Esta garantía se logra mediante el formato PKCS#10 que incluye en la propia solicitud una firma electrónica de la misma, realizada con la clave privada correspondiente a la clave pública del certificado.

8.2.2 Autenticación de la Identidad de una organización

El PSC y/o Casos Especiales deben presentar la solicitud de acreditación ante SUSCERTE con los siguientes recaudos e información:

- Identificación completa del solicitante (PSC y Casos Especiales).
- Información económica y financiera, con la cual se demuestre la capacidad suficiente para prestar servicios (PSC).
- Copia de los contratos correspondientes a aquellos servicios que sean prestados por terceros, en caso de haberlos (PSC).
- Proyectos de contratos a ser suscritos con los signatarios (PSC).
- Política de certificados y Declaración de Prácticas de

Certificación (PSC y Casos Especiales).

- Estados financieros auditados y declaraciones del impuesto sobre la renta de los dos últimos ejercicios fiscales. (PSC)
- Informe de auditoría de acuerdo con lo establecido en el artículo 5 del LSMDFE, elaborado por auditores independientes, no vinculados e inscritos en el registro que a tal efecto lleva SUSCERTE.
- Documento con la descripción detallada de la infraestructura, planes y procedimientos establecidos en el Capítulo VIII del RPLSMDFE. En caso que toda o parte de la infraestructura sea prestada por un tercero debe incluirse copia de los contratos o convenios con éste (PSC y Casos Especiales).

Para facilitar la organización de los recaudos que el PSC debe presentar ante SUSCERTE, se tiene la Norma 027 Guía para la Acreditación de Proveedores de Servicios de Certificación, la cual especifica la documentación requerida clasificada según sea de tipo legal, económica-financiera, técnica o de auditoría.

La autenticación requerirá la presencia física de los representantes de la organización del PSC, de acuerdo a la norma de SUSCERTE llamada Procedimiento de entrega de la credencial al representante legal del solicitante.

Dichas normas se encuentran disponible en el sitio Web http://ww.suscerte.gob.ve/ en la sección de Certificación electrónica específicamente en el enlace llamado: Normativa.

Posterior a la verificación de sus datos y previo a la emisión del certificado, se requerirá del PSC la firma de un contrato con SUSCERTE.

8.2.3 Comprobación de las facultades de representación

La comprobación de la representación del PSC ante SUSCERTE se debe realizar mediante la comprobación de un documento legal, establecidos en la LSMDFE, que lo califique como representante legal. SUSCERTE emitirá una credencial al representante legal el cual le permitirá realizar las solicitudes de acreditación ante SUSCERTE.

8.2.4 Criterios para operar con AC externas

La AC Raíz podrá operar con AC externas siempre que se garantice la acreditación de la AC conforme a lo previsto a la ley de su país. Garantizando así los requisitos de seguridad, validez y vigencia del certificado.

8.3 Identificación y autenticación de solicitudes de renovación de clave

8.3.1 Para las renovaciones rutinarias

La identificación y autenticación para la renovación del certificado se debe realizar utilizando las técnicas para la autenticación e identificación inicial. Este método de renovación requiere que la clave privada no este ni vencida ni revocada.

8.3.2 Para las renovaciones de la clave después de una revocación – clave no comprometida

La política de identificación y autenticación para la renovación de un certificado después de una revocación sin compromiso de la clave será la misma que para el registro inicial. Adicionalmente el PSC y Casos Especiales deberán demostrar satisfactoriamente a SUSCERTE que las causas de revocación anteriores ya no están presentes en su ICP.

SUSCERTE puede negar discrecionalmente la renovación extraordinaria de un certificado para PSC y Casos Especiales.

8.4 Identificación y autenticación de las solicitudes de revocación de la clave

La política de identificación para las solicitudes de revocación podrá ser la misma que para el registro inicial. La política de autenticación acepta solicitudes de revocación firmadas digitalmente por el subscriptor del certificado o de forma manual en las instalaciones de SUSCERTE.

Las Política de certificados de los PSC y Casos Especiales pueden definir otras políticas de identificación siempre y cuando se garantice la posibilidad de autenticación de identidad de acuerdo a la LSMDFE y su Reglamento Parcial.

La AC Raíz o cualquiera de las autoridades que la componen pueden solicitar de oficio la revocación de un certificado si tuvieran el conocimiento o sospecha del compromiso de la clave privada del subscriptor, o cualquier otro hecho que recomendara emprender dicha acción.

9. EL CICLO DE VIDA DE LOS CERTIFICADOS PARA PSC Y CASOS ESPECIALES

9.1 Solicitud de Certificados

Los procedimientos operativos establecidos por SUSCERTE para la acreditación es responsabilidad de los PSC y/o Casos especiales aspirantes a la acreditación. Este proceso se puede llevar a cabo de forma manual dirigiéndose ante las oficinas de SUSCERTE o a través del sistema automatizado visitando la dirección electrónica http://www.suscerte.gob.ve/.

La acreditación de los PSC y/o Casos especiales establece que los mismos operan en conformidad con las políticas y procedimientos establecidos por SUSCERTE.

9.1.1 Autoridades que pueden solicitar acreditación

Todas las entidades públicas y privadas del estado venezolano que cumplan con los requisitos solicitados por SUSCERTE podrán solicitar la acreditación a la cadena de confianza.

Los lineamientos exigidos por la ley sobre mensajes de datos y firmas electrónicas son:

- Capacidad económica y financiera suficiente para prestar los servicios autorizados como PSC. En el caso de organismos públicos, éstos deberán contar con un presupuesto de gastos y de ingresos que permitan el desarrollo de esta actividad.

- Capacidad y elementos técnicos necesarios para proveer Certificados Electrónicos.

- Garantizar servicio de revocación o cancelación, rápido y seguro, de los Certificados Electrónicos que proporcione.

- Sistema de información de acceso libre, permanente, actualizado y eficiente. En el cual se publicarán las políticas y procedimientos aplicados para la prestación de sus servicios, así como los Certificados Electrónicos que hubiere proporcionado, revocado, suspendido o cancelado y las restricciones o limitaciones aplicables a éstos.

- Garantizar que en la emisión de los Certificados Electrónicos que provea se utilicen herramientas y estándares adecuados a los usos internacionales, que estén protegidos contra su alteración o modificación, de tal forma que garanticen la seguridad técnica de los procesos de certificación.

- En caso de personas jurídicas, éstas deberán estar legalmente constituidas de conformidad con las leyes del país de origen.

- Personal técnico adecuado con conocimiento especializado en la materia y experiencia en el servicio a prestar.

- Las demás que señale el reglamento de la LSMDFE.

9.1.2 Proceso de acreditación y responsabilidades PSC

A continuación se describe el proceso de acreditación y sus responsables:

RESPONSABLE	ACCION
SOLICITANTE	1. Recaba en el sitio web de SUSCERTE (www.suscerte.gob.ve) o en sus oficinas, los requisitos para obtener la acreditación como PSC.
AUDITOR	2. Efectúa la auditoría respectiva, emitiendo informe
SOLICITANTE	3. Entrega solicitud de acreditación llena y recaudos de tipo: legal, económico-financiero, técnico y de auditoría
SUSCERTE	4. Recibe solicitud de acreditación y recaudos clasificados 5. Verifica que los recaudos estén completos a) Si los recaudos están completos i) Admite solicitud de acreditación ii) Envía notificación al solicitante Si faltan recaudos: iii) Se indica al solicitante recaudo faltante iv) Ir al paso 3 6. Evalúa si el solicitante cumple todos los requisitos exigidos para acreditarlo a) Si cumple los requisitos: i) La acreditación es aprobada por el Directorio ii) Envía notificación de aprobación al solicitante b) Si no cumple los requisitos: i) La acreditación es negada por el Directorio ii) Envía notificación al solicitante iii) Finaliza el proceso
SOLICITANTE	7. Recibe notificación de aprobación 8. Tramita y envía las garantías que le exige la LSMDFE y su Reglamento Parcial.
SUSCERTE	9. Recibe las garantías constituidas a) Si las garantías corresponden con el modelo presentado y aprobado en los recaudos: i) Ir al paso 10

	Si las garantías no corresponden con el modelo presentado y aprobado en los recaudos: ii) Se niega la solicitud por el Directorio iii) Finaliza el proceso
SOLICITANTE	10. Deposita en la entidad bancaria indicada por SUSCERTE, la tasa correspondiente para la acreditación 11. Envía comprobante de depósito a SUSCERTE
SUSCERTE	12. Emite Providencia Administrativa con la acreditación del solicitante como PSC y/o Casos Especiales, publicándola en la Gaceta Oficial de la RBV. 13. Emite certificado raíz 14. Finaliza el proceso

9.2 Tramitación de solicitud de un certificado

9.2.1 Realización de las funciones de identificación y autenticación

Las funciones de identificación y autenticación las realizan los funcionarios y personal encargado de la operación de los sistemas de acreditación de SUSCERTE.

Estos funcionarios desempeñan el rol de operador de registro, disponiendo de un dispositivo seguro de creación de firma (tarjeta de funcionario) para el control de acceso a la aplicación de expedición y control de integridad y no repudio de las operaciones y transacciones realizadas.

9.2.2 Aprobación o denegación de certificado

Se aprobará las solicitudes de certificación a aquellos proveedores y/o casos especiales, que cumplan con todos los requisitos y lineamientos

técnicos, económicos y legales exigidos por SUSCERTE en la presente DPC. El sistema garantiza que el certificado emitido este dentro de la cadena de confianza de la Infraestructura Nacional de Certificación Electrónica .

9.2.3 Plazo para la tramitación de un certificado

La Superintendencia de Servicios de Certificación Electrónica, previa verificación de los documentos de solicitud para la acreditación deberá pronunciarse sobre la acreditación del Proveedor de Servicios de Certificación, dentro de los veinte (20) días hábiles siguientes a la fecha de presentación de la solicitud.

9.3 Emisión de Certificado

Luego de verificar y aprobar las exigencias establecidas en la LSMDFE el sistema de la AC procederá a realizar la emisión del certificado al PSC y/o Casos Especiales si así lo requiere y es de interés nacional, mediante la publicación en la Gaceta Oficial de la República Bolivariana de Venezuela.

9.3.1 Acciones de la AC durante la emisión del certificado

La emisión de los certificados implica la autorización de la solicitud por parte del sistema de la AC Raíz. Después de la aprobación de la solicitud se procederá a la emisión de los certificados de forma segura y se pondrán los certificados a disposición del PSC y/o Casos Especiales.

En la emisión de los certificados la AC:

- Utiliza un procedimiento de generación de certificados que vincula de forma segura el certificado con la información de registro, incluyendo la clave pública certificada.
- Protege la confidencialidad e integridad de los datos de registro.

Todos los certificados iniciarán su vigencia en el momento que se indica en el propio certificado. Se utilizará el campo de "not before" con este fin. Ningún certificado será emitido con un periodo de validez que se inicie con anterioridad de la fecha actual. Sin embargo, si se podrán emitir certificados cuyo periodo de validez se inicie en el futuro o una fecha posterior a la actual.

9.3.2 Notificación al solicitante por parte de la AC Raíz acerca de la emisión de su certificado

El PSC y/o Casos Especiales sabrán sobre la emisión efectiva del certificado por medio de una carta al representante legal emitido por SUSCERTE. Así mismo, se publica en el diario de mayor circulación nacional, la autorización para que el solicitante comience a actuar como PSC.

9.4 Aceptación de Certificados

9.4.1 Forma en la que se acepta el certificado

El certificado emitido por la AC Raíz al PSC y/o Casos Especiales se considera aceptado luego de su publicación en el repositorio de

Infraestructura Nacional de Certificación Electrónica .

9.4.2 Publicación del certificado por la AC

SUSCERTE provee diversos tipos de comunicación como correos electrónicos, comunicaciones escritas, repositorio LDAP, repositorio Web, OCSP, Gaceta Oficial y los que considere pertinentes para publicar la aceptación de un certificado.

9.4.3 Notificación de la emisión del certificado por la AC a otras Autoridades

SUSCERTE debe notificar a las entidades, organismos del gobierno y empresas privadas la emisión de un certificado por medio del sitio Web de SUSCERTE, el diario de mayor circulación nacional y por la Gaceta Oficial de la República Bolivariana de Venezuela.

9.5 Uso del par de claves y del certificado

El uso de los certificados emitidos por la AC Raíz de Venezuela son los previstos en la LSMDFE y en su Reglamento Parcial.

9.5.1 Uso de la clave privada del certificado por el PSC y/o Casos Especiales

El titular sólo puede utilizar la clave privada y el certificado para los usos autorizados en esta DPC. SUSCERTE emite certificados con los campos de uso de clave privada limitados a firma de certificados y firma de LCR.

9.5.2 Uso de la clave pública y del certificado por los terceros de buena fe

Los terceros de buena fe sólo pueden depositar su confianza en los certificados para aquello que establece esta DPC.

Los terceros de buena fe pueden realizar operaciones de clave pública de manera satisfactoria confiando en el certificado emitido por la cadena de confianza. Así mismo, deben asumir la responsabilidad de verificar el estado del certificado utilizando los medios que se establecen en esta DPC.

9.6 Renovación de certificado con cambio de clave

9.6.1 Causas para la renovación de un certificado

La causa de la renovación de un certificado por parte del PSC, es por la caducidad. Para los Casos Especiales es según lo que establezca su DPC

9.6.2 Entidad que puede solicitar la renovación del certificado

Las entidades autorizadas para solicitar la renovación de un certificado con cambio de clave de un PSC y/o Casos Especiales de la Infraestructura Nacional de Certificación Electrónica de Venezuela:

- El Proveedor de Servicio de Certificación
- La Autoridad para Casos Especiales
- La Autoridad de Certificación Raíz

9.6.3 Procedimiento de solicitud para la renovación de un certificado PSC

El PSC debe cumplir nuevamente con el proceso de acreditación para solicitar la renovación de un certificado. Por tal motivo, el procedimiento de

solicitud para la renovación de un certificado es el mismo que el de acreditación, el cual se describe en el apartado 9.1.2.

9.6.4 Notificación de la emisión de un nuevo certificado al PSC y/o Casos Especiales

SUSCERTE debe notificar al PSC y/o Casos Especiales sobre la emisión efectiva de un nuevo certificado por medio de una carta al representante legal emitido por el Directorio de la Superintendencia. Así mismo, se publica en el diario de mayor circulación nacional.

9.6.5 Publicación del certificado renovado por la AC

SUSCERTE proveerá diversos tipos de comunicación como correos electrónicos, comunicaciones escritas, repositorio LDAP, repositorio Web, OCSP, Gaceta Oficial y los que considere pertinentes para publicar la renovación de un certificado.

9.6.6 Notificación de la emisión del certificado por la AC a otras entidades

SUSCERTE notificará a las entidades, organismos del gobierno y empresas privadas la renovación de un certificado por medio del sitio Web de SUSCERTE, el diario de mayor circulación nacional y por la Gaceta Oficial de la República Bolivariana de Venezuela.

9.7 Modificación de certificados

Durante el ciclo de vida de un certificado, no esta determinado efectuarse la modificación de los campos en la AC Raíz, en los PSC y/o Casos Especiales.

9.8 Revocación y suspensión de un certificado

9.8.1 Circunstancias para la revocación del certificado del PSC y/o Casos Especiales

Las circunstancias para la revocación de un certificado del PSC y/o Casos Especiales son las siguientes:

- Compromiso de la clave privada de la AC Raíz.
- Compromiso o sospecha de la clave privada asociada al certificado del PSC y/o Casos Especiales.
- Cuando el PSC y/o Casos Especiales solicite a la AC Raíz, la suspensión temporal de su certificado.
- Por resolución judicial o administrativa que lo ordene.
- Por la variación de los datos del certificado.

9.8.2 Entidad que puede solicitar la revocación

Al verse comprometida la clave del PSC y/o Casos Especiales, se rompe la cadena de confianza, en esos casos, las entidades autorizadas para solicitar la revocación de acreditación de un PSC y/o Casos Especiales de la Infraestructura Nacional de Certificación Electrónica de Venezuela son:

- La autoridad competente a la conformidad con la LSMDFE
- El PSC y/o Casos Especiales
- La AC Raíz

9.8.3 Procedimiento de solicitud para la revocación

Los pasos para la revocación de la acreditación de un PSC y/o Casos Especiales ante SUSCERTE, son los siguientes:

RESPONSABLE	ACCION
SUSCERTE	1. El Directorio de SUSCERTE determina la suspensión de la acreditación de un PSC y/o Casos Especiales
PSC	2. Recibe la notificación de suspensión de la acreditación como PSC y/o Casos Especiales, resuelta por el Directorio de SUSCERTE 3. Suspende de inmediato la negociación con nuevos usuarios, manteniendo el servicio de los signatarios existentes hasta nuevo aviso 4. Decide acción para solventar la problemática, en función del razonamiento dado por el Directorio de SUSCERTE a la suspensión a. Acata medida por estar de acuerdo con la misma b. Objeta decreto de suspensión de su acreditación, exponiendo el planteamiento ante el Directorio de SUSCERTE
SUSCERTE	5. El Directorio de SUSCERTE conviene con el PSC y/o Casos Especiales las acciones a llevar a cabo, de acuerdo a su planteamiento: a. Acuerda el mecanismo para activar suspensión de la que fue objeto, en el lapso de los quince (15) días que tiene para ello b. Recibe fundamentos del PSC y/o Casos Especiales en contra de la suspensión de la acreditación, utilizando los diez (10) días que la LOPA le asigna para exponer alegatos
PSC	6. Ejecuta las acciones convenidas con el Directorio de SUSCERTE a. Envía a SUSCERTE Plan de Mejoras para solventar la problemática que originó la suspensión de su acreditación b. Remite a SUSCERTE informe justificando las razones de su desacuerdo ante suspensión de la

	acreditación
SUSCERTE	7. Admite los documentos del PSC y/o Casos Especiales a. Ajusta y aprueba el Plan de Mejoras del PSC y/o Casos Especiales i. Autoriza su aplicación en un tiempo determinado, apoyando su ejecución para solucionar el estado de suspensión de la Acreditación b. Analiza el reclamo interpuesto por el PSC y/o Casos Especiales i. Reafirma la suspensión para la acreditación, al comprobar nuevamente los incumplimientos que la originaron ii. Reajusta decisión, si los alegatos del PSC y/o Casos Especiales tienen fundamento, reactivando la acreditación por medio de una Resolución 8. Envía comunicación informativa al PSC y/o Casos Especiales.
PSC	9. Recibe notificación a. Ejecuta Plan de Mejoras b. Resuelve con relación a su reclamo: i. Elaborar un Plan de Mejoras, para evitar la revocación de su acreditación, en el tiempo que le queda para ello ii. O Reiniciar sus actividades ordinarias 10. Informa a SUSCERTE resultado de su gestión
SUSCERTE	11. Periódicamente verifica la situación del PSC y/o Casos Especiales en relación con el estado de la suspensión de la acreditación y

	las acciones en ejecución 12. Si el PSC y/o Casos Especiales cumple con todos los requisitos y obligaciones exigidos por el Decreto-Ley 1.204, su Reglamento Parcial y Normas de SUSCERTE a. Se le reactiva la acreditación b. Se le revoca la renovación de acreditación 13. Finaliza el proceso

9.8.4 Período de gracia de la solicitud de revocación

La revocación se llevará a cabo luego de la tramitación de cada solicitud verificada como válida. SUSCERTE, no contempla ningún período de gracia asociado a este proceso en el que se pueda anular la solicitud de revocación.

9.8.5 Circunstancias para la suspensión

Las circunstancias para la suspensión de un certificado de PSC y/o Casos Especiales, son las siguientes:

- Compromiso de la clave privada de la AC Raíz.
- Compromiso o sospecha de la clave privada asociada al certificado del PSC y/o Casos Especiales.
- Cuando el PSC y/o Casos Especiales solicite a la AC Raíz, la suspensión temporal de su certificado.
- Cuando el PSC y/o Casos Especiales tenga conocimiento del uso indebido de la Firma Electrónica.
- Por resolución judicial o administrativa que lo ordene.
- Por la variación de los datos del certificado.

9.8.6 Entidad que puede solicitar la suspensión

Las entidades autorizadas para solicitar la suspensión de acreditación de un PSC y/o Casos Especiales de la Infraestructura Nacional de Certificación Electrónica de Venezuela:

- La autoridad competente a la conformidad con la LSMDFE
- El PSC
- Caso Especial
- La AC Raíz

9.8.7 Procedimiento para la solicitud de suspensión (temporal)

Los pasos para la solicitud de suspensión del servicio del PSC y/o Casos Especiales ante SUSCERTE, son:

RESPONSABLE	ACCION
SUSCERTE	1. Recibe del PSC y/o Casos Especiales, con la antelación prevista, el plan de mantenimiento y/o mejoras a sus instalaciones, equipos y sistemas, anexando el cronograma de suspensión temporal del servicio por tales actividades. 2. Revisa la planificación de las actividades y el cronograma de suspensión temporal para comprobar la correspondencia entre ambos, siempre pendiente de no permitir que se exceda de los lapsos previstos. 3. Solicita al PSC y/o Casos Especiales ajuste la planificación y el cronograma, de no estar conforme. 4. Aprueba el plan y el cronograma, cuando estos se

	adecuen a las disposiciones del Decreto-Ley 1.204 y a las normativas internas de SUSCERTE. 5. Envía al PSC y/o Casos Especiales el plan y el cronograma de suspensión del servicio temporal aprobados, autorizándolo para ejecutar dicha suspensión en la fecha y hora programada, por el período aceptado.
PSC	6. Recibe de SUSCERTE el plan y el cronograma de suspensión del servicio aprobado. 7. Envía a sus signatarios el cronograma de suspensión del servicio, aprobado por SUSCERTE. 8. Remite a SUSCERTE ejemplar de la notificación con la cual informó a sus signatarios del cronograma de suspensión del servicio.
SUSCERTE	9. Recibe un ejemplar de la notificación donde los signatarios del PSC y/o Casos Especiales son informados del cronograma de suspensión temporal del servicio. 10. Queda pendiente de controlar las acciones a realizar por el PSC y/o Casos Especiales para suspender el servicio, en la fecha y hora aprobadas.
PSC	11. Envía comunicación a sus signatarios donde les recuerda de la fecha y hora de la suspensión del servicio.
PSC	12. Remite ejemplar a SUSCERTE de la notificación enviada a sus signatarios. 13. Suspende el servicio en su oportunidad, en la fecha y hora establecidas. 14. Reinicia el servicio, cumpliendo con el lapso aprobado para la suspensión. 15. Informa a sus signatarios del reinicio del servicio. 16. Despacha a SUSCERTE un ejemplar de la notificación del reinicio del servicio que enviado a sus signatarios.
SUSCERTE	17. Recibe del PSC y/o Casos Especiales copia de la notificación del reinicio del servicio. 18. Constata cumplimiento de la programación establecida.

	19. Participa al PSC y/o Casos Especiales la adecuada aplicación de las disposiciones legales y normativas de SUSCERTE. 20. Fin del proceso.

9.8.8 Límites del período de suspensión

El límite establecido por SUSCERTE para la suspensión de un certificado debe ser no mayor a cuarenta y ocho horas (48) horas.

9.8.9 Frecuencia de emisión de LCR

La AC Raíz, dispone de un servidor Web, accesible desde Internet para cualquiera que necesite consultarlo. El acceso a la información del servidor está disponible 24 horas al día, 7 días a la semana.

Los certificados revocados permanecen insertados en la LCR hasta la fecha de caducidad que se especificó en su emisión.

La frecuencia de emisión de cada LCR es cada vez que se revoque un certificado.

La LCR indica la fecha de publicación de la siguiente lista y sus puntos de distribución específicos. La LCR es emitida y firmada por la AC Raíz.

9.8.10 Requisitos de comprobación de LCR

La información relativa al estado de los certificados LCR de los PSC y/o Casos Especiales se encuentra disponible en la

siguiente dirección: http://acraiz.suscerte.gob.ve/

9.8.11 Disponibilidad de comprobación on-line de revocación

La AC Raíz posee un servidor OCSP para la verificación on-line del estado de los certificados. El repositorio en donde se puede realizar la comprobación en línea esta descrita en el apartado 9.8.10.

9.8.12 Requisitos de comprobación on-line de revocación

El servidor OCSP es de libre acceso y no existe ningún requisito para su uso excepto los derivados del uso del propio protocolo OCSP según se define en el RFC 2560.

La AC Raíz también dispone de un repositorio para la consulta del estado de validez de los certificados expedidos.

9.8.13 Otras formas de divulgación de información de revocación disponibles

A través de la dirección electrónica ldap://acraiz.suscerte.gob.ve y en la Gaceta Oficial de la Republica Bolivariana de Venezuela.

9.9 Servicios de comprobación de estado de certificados

9.9.1 Características Operativas

Para la validación de los certificados electrónicos se dispone de varios prestadores de Servicios de Validación que proporcionan información sobre el estado de los certificados emitidos por la

jerarquía de certificación. Se trata de un servicio de validación en línea (Autoridad de Validación, AV) que implementa el Online Certificate Status Protocol siguiendo la RFC 2560.

Mediante el uso de ese protocolo se determina el estado actual de un certificado electrónico sin requerir las LCR. Un cliente de OCSP envía una petición sobre el estado del certificado a la AV, la cual, tras consultar su Base de Datos, ofrece una respuesta sobre el estado del certificado vía HTTP.

9.9.2 Disponibilidad del Servicio

El servicio de comprobación de estado de certificados está utilizable de forma interrumpida todos los días del año.

9.9.3 Características adicionales

Para hacer uso del Servicio de validación en línea es responsabilidad del tercero de buena fe disponer de un Cliente OCSP que cumpla la RFC 2560.

9.10 Finalización de la suscripción

La finalización de la suscripción de un certificado se produce en los siguientes casos:

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

9.11 Custodia y recuperación de la clave

9.11.1 Prácticas y políticas de custodia y recuperación de la clave

La clave privada de la AC Raíz se custodia por un dispositivo criptográfico HSM. Para el acceso al repositorio de claves privadas se usa el esquema umbral limite (k,n) de Shamir tanto en software como en dispositivos criptográficos.

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

10.1 Controles de Seguridad Física

10.1.1 Ubicación y construcción

Todas las operaciones críticas de la AC Raíz están protegidas físicamente con todas las medidas de seguridad necesarias para los elementos más críticos y con vigilancia durante las 24 horas al día, los 7 días a la semana. Estos sistemas están separados de otros de SUSCERTE, de forma que sólo el personal autorizado pueda acceder a ellos.

El Centro de Procesos de Datos de la AC Raíz cumplen los siguientes requisitos físicos:

- Para evitar posibles daños, las instalaciones se encuentran alejadas de salidas de humos.
- No posee ventanas al exterior de la torre.
- Circuito cerrado de televisión en las áreas críticas o de acceso restringido.

- Control de acceso biométrico.
- Sistemas de detección y extinción de incendios: detectores, extintores, formación del personal para actuar ante incendios, etc.

10.1.2 Acceso Físico

El acceso físico a las instalaciones de la AC Raíz, están protegidas por diversos controles de acceso, de modo que sólo el personal autorizado puede acceder a las mismas. Los controles de acceso, zonas y procesos están definidos en las políticas de seguridad.
Los sistemas de la AC Raíz estarán físicamente separados de otros sistemas de SUSCERTE de forma que únicamente el personal autorizado pueda acceder a ellos, y se garantice la independencia de los otros sistemas informáticos.

Se registra la fecha, hora de entrada y de salida, así como la actividad realizada por todas las personas que acceden al centro de cómputo.

10.1.3 Alimentación eléctrica y aire acondicionado

Las estancias donde están ubicados los equipos cuentan con las condiciones de potencia y ventilación necesarias para evitar fallos de potencia u otras anomalías eléctricas o en los sistemas eléctricos.

El cableado de los equipos está protegido para evitar daños y se han adoptado medidas especiales para evitar las pérdidas de información provocadas por la interrupción en el flujo de suministro eléctrico, conectando los componentes más críticos a fuentes de alimentación

interrumpida (UPS) para asegurar un suministro continuo de energía eléctrica, con una potencia suficiente para mantener la red eléctrica durante los apagados controlados del sistema y para proteger a los equipos frente fluctuaciones eléctricas que los pudieran dañar.

Los sistemas de aire acondicionado conserva las estancias de los equipos con las condiciones de humedad y temperatura adecuadas para el correcto funcionamiento y mantenimiento de los mismos.

10.1.4 Exposición de agua

La instalación de la AC Raíz, esta protegida para evitar las exposiciones al agua de los mismos, mediante detectores de humedad, inundación y otros mecanismos de seguridad apropiados al medio.

10.1.5 Protección y prevención de incendios

La instalación de la AC Raíz, cuenta con sistema inteligente de detección y extinción de incendios.

10.1.6 Sistemas de almacenamiento

La información relacionada a la infraestructura de la AC Raíz se almacena de forma segura en armarios ignífugos y cajas fuertes, según la clasificación de la información en ellos contenida.

10.1.7 Eliminación de residuos

La AC Raíz mantiene mecanismos de revisión por personal autorizado de todos los materiales desechables donde se almacena información

(cdrom, papel, películas). Estos son verificados, antes de su eliminación o reutilización, con el objeto de comprobar si contienen información sensible, siendo físicamente destruidos, salvo que puedan reutilizarse como medio de soporte, en cuyo caso se elimina la información de manera segura.

10.1.8 Almacenamiento de copias de seguridad

Todas las copias de seguridad son almacenadas en entidades distantes a la AC Raíz. Estas dependencias están protegidas con medios y mecanismos de seguridad, apegadas a buenas prácticas internacionales de seguridad.

10.2 Controles Funcionales

10.2.1 Papeles de confianza

La AC Raíz, cuenta con un personal que por sus responsabilidades son sometidos a procedimientos de control especiales debido a que su actividad es esencial para el correcto funcionamiento de la Infraestructura Nacional de Certificación Electrónica. Así tienen la consideración de roles de confianza:

- Responsables del par de claves de la AC Raíz.
- Administrador de HSM.
- Usuario ROOTVE.
- Coordinador de Seguridad.
- Auditor Interno.
- Coordinador de Autoridad de Certificación.

- Director del Departamento.

10.2.2 Número de personas requeridas por rol

Como medida de seguridad las responsabilidades están compartidas entre los distintos roles y personas, de modo que la actitud negligente o dolosa de alguno de ellos no afecta gravemente a la actividad de SUSCERTE como AC Raíz.

10.2.3 Identificación y autenticación para cada rol

Los usuarios encargados de cada uno de los roles descritos en los apartados anteriores se autentican mediante la utilización de criptografía fuerte. Esta autenticación se lleva a cabo utilizando claves privadas resguardados por medio de tarjetas inteligentes y/o dispositivos biométricos.

10.3 Controles de Seguridad Personal

10.3.1 Requerimientos de antecedentes, calificación, experiencia y acreditación

El personal que ejecuta actividades en las instalaciones o sistema de la AC Raíz debe poseer la calificación y experiencia en entornos de prestación de servicios de certificación.

10.3.2 Requerimientos de formación

El personal de SUSCERTE debe estar sujeto a la capacitación para el desarrollo de su función dentro de la institución:

- Formación en los aspectos legales básicos relativos a la prestación de servicios de certificación.
- Conciencia sobre la seguridad física, lógica y técnica.
- Servicios proporcionados por la Autoridad de Certificación.
- Operación del software y hardware para cada rol especifico.
- Conceptos básicos sobre ICP.
- Declaración de Prácticas de Certificación y las Política de certificados pertinentes.
- Gestión de incidencias.

10.3.3 Requerimientos y frecuencia de actualización de la formación

SUSCERTE, preverá inducciones al personal ante cambios tecnológicos del entorno, introducción de nuevas herramientas o modificación de procedimientos operativos.

Adicionalmente se llevará a cabo sesiones formativas ante cambios en la Declaración de Prácticas de Certificación,

Política de certificados u otros documentos relevantes al funcionamiento, administración y/o gerencia de la AC Raíz.

10.3.4 Frecuencia y secuencia de rotación de roles

No aplica este apartado

10.3.5 Sanciones por acciones no autorizadas

Las prácticas del personal de SUSCERTE definen el procedimiento sancionador para los empleados que incumplen las mismas, especificando las sanciones por efectuar una acción no autorizada, el uso no autorizado de la autoridad o el uso no autorizado de los sistemas.

En cualquier caso si SUSCERTE, sospecha de que algún empleado está efectuando una acción no autorizada, automáticamente suspende su permiso de acceso, con la posibilidad de abrirle un proceso de destitución de la institución, de conformidad con el ordenamiento jurídico vigente.

10.3.6 Documentación proporcionada al personal

SUSCERTE, proporciona a sus empleados toda la documentación necesaria para el correcto desempeño de sus tareas. Entre la documentación provista se encuentran:

- Declaración de Prácticas de Certificación
- Manuales de Operación, administración, instalación y utilización de herramientas de la AC Raíz.
- Normas y planes de Seguridad
- Procedimientos de emergencia
- Política de certificados
- Política de Seguridad de la Información
- Organigrama y funciones del personal

10.4 Procedimiento de Control de Seguridad

10.4.1 Tipos de eventos registrados

La AC Raíz, almacena registros electrónicos de eventos (logs) relativos a su actividad como AC de la Infraestructura Nacional de Certificación Electrónica .

Estos registros son guardados, de manera automatizada y en los demás casos en formato papel u otros medios. Estos ficheros están a disposición del auditor en los casos en que sea necesario.

10.4.2 Frecuencia de procesado de registros de logs

Las bitácoras se analizan cuando hay eventos extraordinarios. Cada extracción de logs también deja trazas de auditorías para su posterior revisión.

10.4.3 Periodo de retención para los logs de auditoría

La AC Raíz retendrá todos los registros de auditoría generados por el sistema.

10.4.4 Protección de los logs de auditoría

La integridad de las bitácoras de auditorías se protege mediante la firma de cada evento con la clave privada de la persona que lleva a cabo la acción. Adicionalmente estos logs son resguardados con las mismas medidas de seguridad que la información clasificada como confidencial.

10.4.5 Procedimientos de backup de los logs de auditoría

Este apartado no aplica.

10.4.6 Sistema de recopilación de información de auditoría

El sistema de recopilación de información es ejecutado por: sistemas operativos, procesos en la aplicación de la AC Raíz, y por el personal que las opera. Por lo tanto, este sistema es una combinación de procesos automáticos y manuales. Las características de este sistema son las siguientes:

- Permite verificar la integridad de la base de datos.
- Asegura el no repudio por parte de los autores de las operaciones realizadas sobre los datos. Esto se consigue mediante las firmas electrónicas.

- Guarda un registro histórico de actualización de datos, es decir, almacena versiones sucesivas de cada registro resultante de diferentes operaciones realizadas sobre él.

10.4.7 Notificación al sujeto causa del evento

No aplica este apartado.

10.4.8 Análisis de vulnerabilidad

No aplica este apartado.

10.5 Archivo de Informaciones y Registros

10.5.1 Tipo de informaciones y eventos registrados

Respecto al ciclo de vida de las claves de la AC Raíz:

- Generación de las claves de la AC Raíz.
- Instalación de claves criptográficas y sus consecuencias.
- Copia de respaldo de las claves.
- Almacenamiento de las claves.
- Recuperación de claves criptográficas.
- Uso de las claves.
- Destrucción de claves.

Relacionados con el ciclo de vida de los certificados:

- Recepción de solicitudes para certificados.
- Generación de certificados.
- Distribución de las claves públicas.
- Revocación de certificados.
- Solicitudes de validación de certificados y respuestas.

Relacionados con el ciclo de vida de los dispositivos criptográficos:

- Recepción dispositivos.
- Entrada o traslado al lugar de almacenamiento.
- Uso de dispositivos.
- Desinstalación de dispositivos.
- Designación del dispositivo para el servicio o reparación.
- Retirada de dispositivos.

Otros:

- Actualización de la DPC.
- Acuerdos de confidencialidad.
- Accesos y modificaciones de la documentación solicitada por los auditores.
- Convenios suscritos por SUSCERTE.
- Autorización de acceso a los sistemas de información.

10.5.2 Período de retención para el archivo

Las trazas de los archivos son conservadas durante un período de veinte años.

10.5.3 Protección del archivo

Las medidas de seguridad definidas están destinadas a proteger los archivos de accesos (internos o externos) no autorizados, de modo que sólo ciertas personas pueden consultar, modificar o eliminar los archivos. Los archivos son almacenados en lugares seguros, con todas las medias de seguridad necesarias para protegerlos de factores naturales.

10.5.4 Procedimientos de backup del archivo

Este apartado no aplica.

10.5.5 Requerimientos para el estampado de tiempo de los registros

SUSCERTE en estos momentos se encuentra realizando el proyecto para incorporar el estampado de tiempo a la firma electrónica.

10.5.6 Sistema de repositorio de archivos de auditoria (interno vs externo)

El sistema de repositorio de archivos se realiza utilizando medios ignífugos y resistentes al tiempo.

10.5.7 Procedimientos para obtener y verificar información archivada

Sólo el personal autorizado tiene acceso a los archivos físicos de soportes y archivos informáticos, para llevar a cabo verificaciones de integridad u otras.

Esta verificación debe ser llevada a cabo por el Auditor de Sistema que debe tener acceso a las herramientas de verificación y control de integridad del registro de eventos de la ICP. De forma automática se realizan comprobaciones de la integridad de los archivos electrónicos, en tiempo de su generación y se crea una incidencia en el caso de errores o comportamientos imprevistos.

10.6 Cambio de Clave

Las claves de los certificados emitidos por AC Raíz dejarán de tener validez en el mismo momento en que lo haga su certificado autofirmado. Una vez expirado la AC Raíz generará un nuevo par de claves que autofirma para generar el nuevo certificado raíz.

10.7 Continuidad del Negocio y Recuperación ante Desastre

Los requisitos de notificación y los procedimientos de recuperación en caso de compromiso de la clave privada o desastre, los cuales están ampliamente desarrollados en la Norma SUSCERTE052, son los siguientes:

10.7.1 Procedimientos de gestión de incidentes y vulnerabilidades

SUSCERTE tiene establecido un Plan de Continuidad de Negocio y Recuperación ante Desastres, que define las acciones a realizar, recursos a utilizar y personal a emplear en el caso de producirse un acontecimiento intencionado o accidental que inutilice o degrade los recursos y los servicios de certificación prestados por la AC Raíz.

10.7.2 Alteración de los recursos hardware, software y/o datos

La AC Raíz, dispone de un plan de continuidad de negocio y recuperación ante desastres, que le permite seguir operando si el hardware, software y/o los datos son alterados (pero no destruidos). También, actualiza periódicamente este plan con el fin de asegurar su vigencia en todo momento.

El plan incluye los procedimientos necesarios para garantizar la continuidad de la actividad durante el período de tiempo transcurrido entre el desastre y el restablecimiento de la situación original (dando prioridad a la publicación de las LCR).

10.7.3 Procedimiento de actuación ante la vulnerabilidad de la clave privada de una autoridad

El plan de continuidad del negocio y recuperación ante desastres, de la AC Raíz considera el compromiso o sospecha de su clave privada como un desastre. En este caso, prevé la publicación y difusión, inmediatamente, de la revocación de su certificado con el objeto de impedir la confianza en el mismo.

10.7.4 Seguridad de las instalaciones tras un desastre natural o de otro tipo.

La AC Raíz, dispone de ubicaciones externas para mantener almacenadas las copias de seguridad, para minimizar los efectos en caso de desastre natural o de otro tipo sobre las instalaciones primarias.

10.8 Cese de la actividad

La AC Raíz, no podrá notificar la culminación de sus actividades de servicios de certificación. Por su naturaleza de AC Raíz de la jerarquía de confianza de la Infraestructura Nacional de Certificación Electrónica del país, en caso de tener comprometida su clave deberá inmediatamente crear un nuevo certificado electrónico autofirmado y firmar los certificados vigentes de los PSC acreditados.

11. CONTROLES DE SEGURIDAD TÉCNICA

11.1 Generación e instalación de par de claves

11.1.1 Generación del par de claves

La AC Raíz, genera el par de claves (Pública y Privada) utilizando un dispositivo de hardware criptográfico (HSM) que cumple con los requisitos establecidos en un perfil de protección de dispositivo seguro de firma electrónica de autoridad de certificación normalizado, de acuerdo con FIPS

140-2 Nivel 3 o superior nivel de seguridad.

El procedimiento de generación de las claves para los PSC acreditados ante SUSCERTE es idéntico, en su propio HSM.

11.1.2 Entrega de la clave privada al PSC

El PSC es responsable de la generación de su par de claves y por lo tanto responsable de su resguardo y custodia.

11.1.3 Entrega de la clave pública al PSC

Las claves públicas generadas bajo el control de los PSC se envían a SUSCERTE como parte de una solicitud de acreditación. Esta solicitud se realiza en formato PKCS#10, firmado digitalmente con la clave privada correspondiente a la clave pública que se solicita certificar.

11.1.4 Disponibilidad de la clave pública

La clave publica de la AC Raíz estará disponible en http://acraiz.suscerte.gob.ve las 24 horas del día los 7 días de la semana de forma continua.

11.1.5 Tamaño de las claves

Los algoritmos criptográficos empleados por la AC Raíz para firmar los certificados y las LCR son SHA1wihtRSA,

SHA256withRSA y SHA384withRSA. La longitud de la clave con el algoritmo RSA de la AC Raíz y del PSC es de 4096 bits.

El Uso de Sha1withRSA se permite temporalmente por motivos de interoperabilidad con sistemas que no soportan Sha256withRSA ó Sha384withRSA. Se estima que en diciembre del año 2011 se revisará la DPC para excluir Sha1withRSA.

11.1.6 Parámetros de generación de la clave pública y verificación de la calidad

La AC Raíz, los PSC y/o Casos Especiales, deben generar sus pares de claves de acuerdo con RFC 3280 y PKCS#1. El algoritmo de generación de claves es el RSA. La verificación de la calidad se realiza de acuerdo con el informe especial del ETSI SR 002 176, que indica la calidad de los algoritmos de firma electrónica.

Los algoritmos y parámetros de firma utilizados por la AC raíz, PSC y/o Casos Especiales para la firma de certificados electrónicos y listas de certificados revocados son los siguientes:

- Algoritmo de firma: RSA
- Parámetros del algoritmo de firma: Longitud del Módulo=4096

- Algoritmo de generación de claves: rsagen1
- Método de relleno: emsa-pkcs1-v1_5
- Funciones criptográficas de Resumen: SHA-1/SHA-256/SHA-384

11.1.7 Hardware/Software de generación de claves

La AC Raíz, genera su par de claves utilizando un módulo de hardware criptográfico (HSM). La autenticación contra el HSM requiere de al menos 2 de 3 operadores. Este procedimiento sigue el esquema umbral límite de Shamir (k,n), con el modo no persistente del dispositivo criptográfico. En este modo es necesario garantizar la conexión física del último juego de tarjetas en el lector del HSM, para abrir la clave privada de la AC Raíz.

11.1.8 Propósitos de utilización de claves

Los certificados emitidos por la AC Raíz incluyen la extensión Keyusage para restringir el propósito de la clave pública del certificado, indicando que la claves solo es para:

- Firma certificado
- Firma LCR

11.2 Protección de la clave privada

La clave privada de la AC Raíz, es protegida por un mundo de seguridad generada por un dispositivo criptográfico. Con la finalidad de mantener el resguardo de las claves privadas del certificado autofirmado, la clave privada nunca se encuentra descifrada fuera del HSM. Las copias de seguridad mantienen el secreto de la clave privada de la misma forma en que se resguarda la clave privada original.

11.2.1 Estándares para los módulos criptográficos

El HSM que utiliza la AC Raíz, para generar sus claves es certificado FIPS 140-2 Nivel 3. La clave pública ha sido almacenada en formato electrónico firmado, de modo que están protegidas de fallos electrónicos y/o problemas con la potencia eléctrica.

Por lo tanto, la puesta en marcha de una AC implica las siguientes tareas:

- Inicialización del estado del módulo HSM.
- Creación de las tarjetas de administración y de operador.
- Generación de las claves de la AC.

11.2.2 Control “N” de “M’ de la clave privada

La clave privada, tanto de la AC Raíz como de los PSC, se encuentra bajo control multipersona. Esta se activa mediante la inicialización del software de AC por medio de

una combinación de operadores de la AC, administradores del HSM y usuarios de Sistema Operativo. Éste es el único método de activación de dicha clave privada.

11.2.3 Custodia de la clave privada

La clave privada de la AC Raíz se encuentra alojada en un dispositivo criptográfico. Cumple con los requisitos establecidos en un perfil de protección de dispositivo seguro de firma electrónica de autoridad de certificación normalizado, de acuerdo con FIPS 140-2 Nivel 3 de seguridad.

Las claves privadas de la AC Raíz y PSC se encuentran alojadas en dispositivos de hardware criptográfico con certificación FIPS 140-2 de nivel 3.

El resto de claves privadas de operadores y administradores se encuentran contenidas en tarjetas inteligentes criptográficas en poder de los administradores de cada autoridad.

11.2.4 Copia de seguridad de la clave privada

Este apartado no aplica.

11.2.5 Archivo de la clave privada

Este apartado no aplica.

11.2.6 Inserción de la clave privada en el módulo criptográfico

Las claves privadas se crean dentro del módulo criptográfico en el momento en que este se inicializa Posteriormente la clave privada generada dentro del HSM es exportada en forma cifrada.

11.2.7 Método de activación de la clave privada

Consiste en la utilización de las tarjetas inteligentes para repartir el acceso en distintas personas y roles. Explícitamente la única combinación para activar la clave privada requiere la presencia de dos de tres administradores del HSM, tres de ocho operadores del HSM y un administrador del Sistema Operativo de la aplicación.

11.2.8 Método de desactivación de la clave privada

Un administrador del Sistema Operativo puede proceder a la desactivación de la clave privada de la AC Raíz. Después de haber sido activada por la combinación descrita en el apartado anterior el operador puede proceder a la desactivación mediante la detención de la aplicación ROOTVE.

11.2.9 Método de destrucción de la clave privada

La AC Raíz eliminará su clave privada cuando expire su plazo de vigencia o haya sido revocada.

La destrucción se realizará utilizando los comandos establecidos para borrar físicamente de la memoria del HSM la parte en la que estaba grabada la clave.

11.2.10 Ránking del módulo criptográfico

El módulo criptográfico utilizado tanto por la AC Raíz como por los PSC debe poseer la certificación FIPS 140-2 nivel 3.

11.3 Otros aspectos de la gestión del par de claves

11.3.1 Archivo de la clave pública

La clave pública de la AC Raíz, es archivada según el formato estándar PKCS#7, por un período de 20 años.

11.3.2 Periodos operativos de los certificados y periodo de uso para el par de claves

El par de claves de la AC Raíz tendrá una validez de veinte (20) años, mientras que el de los PSC tendrá una validez de diez (10) años y el de los Casos Especiales por quince (15) años. Por otro lado los períodos de operación de los certificados serán de la mitad del período de validez.

11.4 Datos de activación

11.4.1 Generación e instalación de datos de activación

Los datos de activación de la AC Raíz y PSC se deben generar y almacenar en tarjetas inteligentes. Su protección se garantiza mediante un PIN (número de identificación personal) en posesión de personal autorizado.

11.4.2 Protección de datos de activación

Sólo el personal autorizado posee las tarjetas criptográficas con capacidad de activación de las claves privadas de la AC, así mismo conocen los PINs necesarios para su utilización.

La clave personal de acceso (PIN) es confidencial, personal e intransferible y es el parámetro que protege las claves privadas permitiendo la utilización de los certificados de AC Raíz y PSC.

11.5 Controles de seguridad del computador

11.5.1 Requisitos Técnicos específicos

SUSCERTE ha definido en el documento de políticas de seguridad, los controles y técnicas aplicables a los equipos informáticos. Estos controles se refieren a aspectos tales como el uso de los equipos, controles de acceso discrecional y obligatorio, auditorías, identificación y

autenticación.

11.5.2 Calificaciones de seguridad computacional

SUSCERTE, utiliza productos certificados, al menos, por el Nivel E3 de las normas ITSEC.

11.6 Controles de seguridad del ciclo de vida

11.6.1 Controles de desarrollo de sistemas

No aplica este apartado

11.6.2 Controles de administración de seguridad

SUSCERTE, debe mantener un inventario de todos los activos informáticos y realizar una clasificación de los mismos de acuerdo con sus requerimientos de protección.

11.6.3 Calificaciones de seguridad del ciclo de vida

Durante todo el ciclo de vida del sistema se debe implementar controles de seguridad que permitan instrumentar y auditar cada fase de los sistemas de la AC Raíz.

11.7 Controles de seguridad de la red

La infraestructura tecnológica de la AC Raíz, no está conectada a la red permanece fuera de línea para garantizar un servicio fiable e

íntegro.

11.8 Controles de ingeniería de los módulos criptográficos

La AC Raíz utiliza módulos criptográficos hardware y software disponibles comercialmente desarrollados por terceros. La AC Raíz únicamente utiliza módulos criptográficos con certificación FIPS 140-2 nivel 3.

12 PERFILES DE CERTIFICADOS, LCR Y OCSP

12.1 Perfil del certificado

Los certificados de la AC Raíz y PSC son emitidos conforme a los siguientes estándares:

- RFC 3280: Internet X.509 Public Key Infrastructure - Certificate and LCR Profile, Abril 2002.
- ITU-T Recommendation X.509 (2005): Information Technology – Open Systems Interconnection - The Directory: Authentication Framework.
- ETSI TS 101 862 V1.3.1 (2004-03): Qualified Certificate Profile, 2004.
- RFC 3739: Internet X.509 Public Key Infrastructure – Qualified Certificate Profile, Marzo 2004 (prevaleciendo en caso de conflicto la TS 101 862).

12.1.1 Número de versión

La AC Raíz, soporta y emite certificados X. 509 versión 3. X.509 es un estándar desarrollado por la Unión Internacional de Telecomunicaciones (Organización Internacional de las Naciones Unidas para coordinación de servicios de redes de telecomunicaciones entre Gobiernos y empresas) para las Infraestructuras de Clave Pública y los Certificados electrónicos.

12.1.2 Extensiones del certificado

Las extensiones del certificado de la AC Raíz permiten codificar información adicional en los certificados.

Las extensiones estándar X.509 definen los siguientes campos:

- SubjectKeyIdentifier
- AuthorityKeyIdentifier
- BasicConstraints. Marcada como crítica
- Certificate Policies. Marcada como crítica
- KeyUsage. Marcada como crítica
- LCRDistributionPoint. Marcada como crítica
- SubjectAlternativeName. Marcada como crítica

12.1.3 Identificadores de objeto (OID) de los algoritmos

Los OID de los algoritmos criptográficos utilizados por la AC

Raíz son:

- SHA1withRSAEncryption (1.2.840.113549.1.1.5)
- SHA256withRSAEncryption (1.2.840.113549.1.1.11)
- SHA384withRSAEncryption (1.2.840.113549.1.1.12)

12.1.4 Formatos de nombres

El certificado de la AC Raíz contiene como DN, en formato X. 500, los nombres del emisor y titular del certificado en los campos emisor (issuer) y sujeto (subject).

12.1.5 Restricciones de los nombres

Los nombres contenidos en los certificados están restringidos a distinguished names X.500, únicos y no ambiguos.

12.1.6 Identificador de objeto (OID) de la Política de Certificación

La AC Raíz tiene definida una política de asignación de OID's dentro de su árbol privado de numeración. El OID de las PC de la AC Raíz es: 2.16.862.1.2

12.2 Perfil de la LCR

12.2.1 Número de versión

La AC Raíz, emite LCR con formato X. 509 v. 2.

12.2.2 Extensiones de las LCR

Las extensiones de las LCR emitidas por la AC Raíz, son las definidas por el IETF en su RFC 2459, es decir:

- Authority Key Identifier
- LCR Number
- Issuing Distribution Point

12.3 Perfil de OCSP

12.3.1 Número de versión

Los certificados de OCSP utilizarán el estándar X.509 versión 3 (X.509 v3)

12.3.2 Extensiones de las OCSP

Las extensiones X509v3 utilizadas en los certificados de OCSP son:

- Subject Key Identifier
- Authority Key Identifier
- KeyUsage
- extKeyUsage
- Certificate Policies
- Policy Identifier

- URL DPC
- Notice Reference
- Basic Constraints
- Subject Type
- Auth Information Access
- OCSPNoCheck

13 AUDITORÍA DE CONFORMIDAD

13.1 Frecuencia de los controles de conformidad para cada entidad

El sistema de acreditación de la AC Raíz se someterá a una auditoría interna de forma anual, de acuerdo con el Plan de Auditorías elaborado por SUSCERTE. De esta manera se garantiza la adecuación de su funcionamiento y operatividad con las estipulaciones incluidas en esta DPC y PC.

Adicionalmente SUSCERTE llevará acabo auditorías internas bajo su propio criterio o en cualquier momento, a causa de una sospecha de incumplimiento de alguna medida de seguridad o por un compromiso de las claves.

Igualmente cada dos (02) años se llevará a cabo una autoría externa para evaluar el grado de conformidad respecto a la especificación técnica ETSI TS 101 456 “Policy requirements for certification authorities issuing qualified certificates”, teniendo en cuenta los

criterios de la CWA 14172-2 ("EESSI Conformity Assessment Guidance - Part 2: Certification Authority services and processes").

13.2 Auditores

El auditor será seleccionado en el momento de la realización de cada auditoría.

Cualquier empresa o persona contratada para realizar una auditoría de seguridad sobre AC raíz, los PSC o los Casos Especiales, deberá cumplir con los siguientes requisitos:

- Estar inscrito en el Registro de Auditores de SUSCERTE (Auditoría Externa).
- Adecuada y acreditada capacitación y experiencia en ICP, seguridad y procesos de auditoría de sistemas de información.
- Independencia a nivel organizativo de la autoridad de AC Raíz, para el caso de auditorías externas.

13.3 Relación entre el auditor y la autoridad auditada

La relación entre el auditor y la autoridad auditada se debe limitar estrictamente a los procesos e información requerida para la auditoría. Por lo tanto la parte auditada (AC Raíz, PSC y/o Casos Especiales), no deberá tener ninguna relación, actual o planificada, financiera, legal, o de cualquier otra clase que pueda derivar en un conflicto de intereses con el auditor. En el caso de los auditores internos, estos no podrán tener relación funcional con el área objeto

de la auditoría.

13.4 Tópicos cubiertos por el control de conformidad

Son objeto de auditoría todos los requisitos técnicos, funcionales y organizativos entre ellos:

- La DPC y PC utilizadas.
- Políticas de Seguridad.
- Administración de la AC Raíz
- Consideraciones de Confidencialidad.
- Seguridad Física.
- Plan de Contingencia y Recuperación ante Desastres.
- Plan de Continuidad de las Actividades.
- Personal Operativo.

13.5 Acciones a tomar como resultado de una deficiencia

La identificación de cualquier anomalía en la auditoría dará lugar a la corrección inmediata de medidas correctivas para ser solventadas en el menor tiempo posible.

En el caso de una deficiencia grave, el Directorio de SUSCERTE podrá determinar la suspensión temporal de las operaciones de la AC Raíz hasta que las deficiencias se corrijan, la revocación del certificado de la autoridad, cambios en el personal, etc.

13.6 Comunicación del resultado

El auditor debe comunicar los resultados de la auditoría al AAP y a

los responsables de las distintas áreas en las que se detecten no conformidades.

14 REQUISITOS COMERCIALES Y LEGALES

14.1 Aranceles

La AC Raíz, de la Infraestructura Nacional de Certificación Electrónica de Venezuela no esta sujeta al pago de aranceles. Solo los PSC acreditados ante SUSCERTE, son los que están obligados a cumplir con las tasas impuestas en la LSMDFE.
Especificado en el Artículo 24 De las tasas del Capítulo V de la Superintendencia de Servicios de Certificación Electrónica de la LSMDFE. Los PSC constituidos por entes públicos de la nación venezolana estarán exentos del pago de las tasas de este artículo.

14.1.1 Tasas de registro para la acreditación o renovación de los PSC.

Los PSC deben pagar, las tasas de registro por la expedición y renovación de acreditación, ante SUSCERTE:

- Por la Acreditación de los PSC, AC Subordinadas de la AC Raíz de Venezuela, SUSCERTE cobrará una tasa de un mil unidades tributarias (1.000 U.T).
- Por la Renovación de la acreditación de los PSC se cobrará una tasa de quinientas unidades tributarias (500 U.T).

14.1.2 Tasas de registro por cancelación de acreditación

Por el pago de la acreditación de los PSC ante SUSCERTE, se cobrará una tasa de quinientas unidades tributarias (500 U.T).

14.1.3 Tasas de registro por los certificados otorgados por PSC extranjeros

Los PSC extranjeros deben cancelar una tasa de quinientas unidades tributarias (500 U.T).

14.1.4 Tarifas de otros servicios como información de políticas

Por el servicio de información sobre la PC, DPC u otros servicios adicionales del que se tenga conocimiento en el momento de la redacción del presente documento, no se aplicará ninguna tarifa.

14.2 Capacidad Financiera

14.2.1 Indemnización a terceros que confían en los certificados emitidos por los PSC

Los PSC deben presentar garantía expedida por una entidad aseguradora o bancaria autorizada para operar en el país, y sus condiciones deben cubrir todos los perjuicios

contractuales y extracontractuales de los signatarios y terceros de buena fe.

14.2.2 Capacidad financiera de los PSC

Según lo que prevé la LSMDFE, los PSC deben poseer capacidad económica y financiera con la cual garanticen la continuidad de los servicios.

14.2.3 Procesos administrativos

SUSCERTE debe garantizar continuas auditorías a los procesos y procedimientos administrativos establecidos de manera regular. Estas auditorías se llevarán a cabo tanto de manera interna como externa.

14.3 Políticas de confidencialidad

La AC Raíz, se compromete a proteger todos los datos a los que tenga acceso como consecuencia de su actividad como AC de la Infraestructura Nacional de Certificación Electrónica de Venezuela.

No obstante, AC Raíz se reserva el derecho a revelar a los empleados y consultores, externos o internos, los datos confidenciales necesarios para realizar sus actividades como AC Raíz. En este caso los empleados y/o consultores son informados

sobre las obligaciones de confidencialidad.

Estas obligaciones no se aplican si la información calificada como "confidencial" es requerida por los Tribunales u órganos administrativos competentes o impuesta por una ley.

14.3.1 Información confidencial

Se considera información confidencial:

- Información de registro, todos los datos relativos al registro de certificados son considerados confidenciales.
- La información de negocio suministrada por sus proveedores y otras personas con las que SUSCERTE tiene el deber de guardar secreto establecida legal o convencionalmente.
- Información sobre la vida de los certificados, todos los datos relativos a la emisión y revocación (salvo su publicación en la LCR) de certificados de los PSC.
- Toda la información clasificada como "Confidencial"

14.3.2 Información no confidencial

Se considera información no confidencial:

- Contenido de los certificados emitidos
- Lista de Certificados Revocados (LCR)
- La clave pública de la AC Raíz

- Las versiones de la DPC
- La Política de Certificados (PC)
- Los siguientes Documentos: plan de contingencia y recuperación ante desastres, plan de seguridad de sistemas y en general cualquier documento que la AC Raíz requiera para su operación.
- La LSMDFE y su Reglamento.
- Toda otra información identificada como "Pública"

14.3.3 Publicación de información sobre la revocación o suspensión de un certificado

La AC Raíz posee un directorio LDAP, el cual actúa como repositorio de la AC Raíz, para la publicación de información relativa a la renovación o suspensión de certificados.

14.3.4 Divulgación de información como parte de un proceso judicial o administrativo

La AC Raíz, puede revelar información calificada como confidenciales a la Autoridad Judicial pertinente que lo requiera formalmente.

14.4 Protección de la información privada/secreta

14.4.1 Información considerada privada

Los siguientes datos son considerados como información privada:

- Solicitudes de certificados, aprobadas o denegadas, así como toda otra información personal obtenida para la expedición y mantenimiento de certificados.
- Claves privadas generadas y/o almacenadas por la AC Raíz.
- Contraseña de acceso personal al sistema de la AC Raíz.
- Todas las claves privadas generadas como un par de clave publica-privada y depositada en una tarjeta inteligente o cualquier otro repositorio.
- Los números de identificación personal (PIN) que protegen las claves privadas en tarjetas inteligentes.
- Toda otra información identificada como “Información privada/secreta”.

Asimismo, los datos captados por el PSC tienen la consideración legal de datos de nivel básico.

14.4.2 Información no considerada privada

La información no tiene carácter privado, por imperativo legal (“datos públicos”), pero solo se publica en el depósito si lo consiente el suscriptor.

En todo caso, es considerada no confidencial la siguiente información:

- Los certificados emitidos o en trámite de emisión
- El nombre y los apellidos del suscriptor del

certificado, así como cualesquiera otras circunstancias o datos personales del titular, en el supuesto que sean significativas en función de la finalidad del certificado, de acuerdo con este documento.

- La dirección electrónica del suscriptor del certificado.
- Los usos y límites económicos reseñados en el certificado.
- El periodo de validez del certificado, así como la fecha de emisión del certificado y la fecha de caducidad.
- El número de serie del certificado.
- Los diferentes estados o situaciones del certificado y la fecha del inicio de cada uno de ellos, en concreto: pendiente de generación y/o entrega, válido, revocado, suspendido o caducado y el motivo que provocó el cambio de estado.
- Las listas de certificados revocados (LCR), así como el resto de informaciones de estado de revocación.
- La información contenida en el Depósito de la AC Raíz.

14.4.3 Responsabilidades de proteger la información privada/secreta

La AC Raíz garantiza el cumplimento de sus obligaciones legales como prestador de servicios de certificación, de

conformidad con la Ley.

14.4.4 Prestación del consentimiento en el uso de la información privada/secreta

La AC Raíz debe obtener el consentimiento de los PSC para utilizar su información privada provista durante el proceso de acreditación. Se entenderá obtenido el consentimiento con la firma del contrato de certificación y la retirada de los certificados por parte del PSC.

14.4.5 Comunicación de la información a autoridades administrativas y/o judiciales

La AC Raíz sólo podrá revelar información calificada como privada/secreta en aquellos supuestos en los que así se le requiera por la autoridad pública competente y en los supuestos previstos legalmente.

14.5 Derechos de propiedad intelectual

La propiedad y los derechos de propiedad intelectual del presente Documento son de la Superintendencia de Servicios de Certificación Electrónica (SUSCERTE).

14.6 Obligaciones y responsabilidad civil

14.6.1 Obligaciones de la Autoridad de Registro

La Autoridad de Registro debe cumplir las siguientes

obligaciones:

- Realizar sus operaciones en conformidad con esta DPC.
- Realizar sus operaciones de acuerdo con la PC que sea de aplicación para los tipos de certificado solicitados en cada caso.
- Comprobar exhaustivamente la identidad de las organizaciones acreditadas para lo que se requerirá la presencia física del representante legal y los documentos necesarios que se describen en esta DPC.
- No almacenar ni copiar datos de creación de firma de las organizaciones a las que hayan acreditado.
- Informar, antes de la acreditación, a la organización solicitante, sobre las obligaciones que asume, entre las cuales se encuentran las siguientes:
  - La forma en que debe custodiar los datos de creación de firma.
  - El procedimiento que debe seguir para comunicar la pérdida o utilización indebida de los datos o dispositivos de creación y de verificación de firma.
  - De su precio.
  - De las condiciones precisas para la utilización del certificado.
  - De sus limitaciones de uso y de la forma en que garantiza su posible responsabilidad

patrimonial.

- Del sitio Web donde puede consultar cualquier información de la AC Raíz, la DPC y las PC vigentes y anteriores.
- La legislación aplicable
- Las certificaciones obtenidas
- Los procedimientos aplicables para la resolución extrajudicial de los conflictos que pudieran surgir por el ejercicio de la actividad.

- Formalizar el Contrato de Certificación con el subscriptor según lo establecido por la Política de Certificados aplicable.
- Solicitar la revocación de un certificado cuando tenga conocimiento o sospecha del compromiso de una clave privada.
- Autentificar las solicitudes de los PSC para la renovación o revocación de sus certificados, generar solicitudes de renovación o revocación firmadas digitalmente.
- En el caso de la aprobación de una solicitud de acreditación notificar al subscriptor la emisión de sus certificados y la forma de obtenerlo.
- En el caso del rechazo de una solicitud de acreditación, notificar al solicitante dicho rechazo y su motivo.
- Mantener bajo su estricto control las herramientas de

tramitación de certificados electrónicos.

- Recibir y tramitar las solicitudes de revocación presenciales que reciba de manera inmediata, después de haber llevado a cabo una identificación fiable de representante legal de la organización, basadas en las normas expresadas en este DPC.

14.6.2 Obligaciones de la Autoridad de Certificación

- Asegurar la protección de la clave privada de la misma AC Raíz.
- Verificar que los PSC y/o Casos Especiales cumplen los requisitos para ser miembros de la jerarquía de confianza de la Infraestructura Nacional de Certificación Electrónica .
- Publicar en el sitio Web de SUSCERTE esta DPC de la AC Raíz.
- Asegurar que su clave pública, la DPC, PC y otros documentos de carácter público, estén disponibles para cualquier interesado que lo requiera.
- Garantizar la adopción de las medidas necesarias para evitar la falsificación de los Certificados Electrónicos y de las Firmas Electrónicas que proporcionen.
- Realizar auditorías internas a la aplicación Infraestructura Nacional de Certificación Electrónica de la AC Raíz al menos una vez al año.

- Revocar o suspender el certificado de un PSC y/o Casos Especiales si se da alguna de las causas expuestas en la LSMDFE, su Reglamento Parcial o la DPC.
- Mantener un registro actualizado de los certificados de los PSC que han sido otorgados, revocados o suspendidos.
- Revocar o suspender aquellos certificados que habiendo sido emitidos, se sospeche o conozca que el secreto de la clave privada ha sido vulnerado.

Conservar toda la información y documentación relativa a los certificados, en medios electrónicos o magnéticos o lo que establezca la legislación vigente, para su consulta durante 20 años.

14.6.3 Obligaciones del Proveedor de Servicios de Certificación

El Proveedor de Servicios de Certificación (PSC) debe:

- Tener conocimiento de los pasos necesarios para la acreditación ante SUSCERTE.
- Actuar con diligencia para evitar el uso no autorizado de su Firma Electrónica.
- Garantizar y proteger sus claves privadas en dispositivos criptográficos que cumplan con la FIPS 140-2 Nivel 3.
- Notificar a la AC Raíz que su Firma Electrónica ha sido controlada por terceros no autorizados o

indebidamente utilizada, cuando tenga conocimiento de ello.

- Mantener el esquema de la arquitectura de ICP con la jerarquía en forma de árbol, para las autoridades que partan de ella.
- Emitir, distribuir, revocar o suspender los certificados de las Autoridades de Certificación Subordinadas al PSC.
- Elaborar su propia DPC y PC.
- Cumplir con el Artículo 35 de las Obligaciones de los Proveedores del Capítulo VI De los Proveedores de Servicios de Certificación de la LSMDFE.

14.6.4 Obligaciones de los terceros de buena fe

Es obligación de los terceros de buena fe que confíen en los certificados emitidos por AC Raíz:

- Limitar la fiabilidad de los certificados a los usos permitidos de los mismos, en conformidad con lo expresado en las extensiones de los certificados y la PC pertinente.
- Verificar la validez de los certificados en el momento de realizar o verificar cualquier operación basada en los mismos.
- Asumir su responsabilidad en la correcta verificación de las firmas electrónicas
- Asumir su responsabilidad en la comprobación de la validez, revocación o suspensión de los certificados

en que confía.

- Tener pleno conocimiento de las garantías y responsabilidades aplicables en la aceptación y uso de los certificados en los que confía, y aceptar sujetarse a las mismas.

14.6.5 Obligaciones del repositorio

- Mantener accesible para todos los participantes de la Infraestructura Nacional de Certificación Electrónica el conjunto de certificados emitidos por la AC Raíz.
- Mantener accesible para todos los participantes de la Infraestructura Nacional de Certificación Electrónica la información de los certificados que han sido revocados, en formato CRL.

14.7 Renuncias de Garantías

La AC Raíz puede rechazar todas las garantías del servicio que no se encuentren vinculadas a obligaciones establecidas por la LSMDFE, especialmente aquellas garantías de adaptación para un propósito particular o garantía de uso mercantil del certificado.

14.8 Limitación de Responsabilidades

La AC Raíz cumple con todas las normas, políticas, lineamientos, estándares internacionales en la materia. Por otro lado los PSC acreditados deben seguir la LSMDFE, su Reglamento Parcial, los

estándares internacionales, las normas y procedimientos de acreditación, auditorías, y otros que SUSCERTE considere necesario.

14.8.1 Deslinde de responsabilidades

SUSCERTE no asume ninguna responsabilidad en caso de pérdida o perjuicio:

- De los servicios que presta, en caso de guerra, huelgas, paros, golpes de estado, desastres naturales o cualquier otro caso de fuerza mayor.
- Ocasionados por el uso de certificados que exceda los límites establecidos por los mismos, la PC y DPC.
- Ocasionado por el uso indebido o fraudulento de los certificados o LCR emitidos por la AC Raíz.
- Ocasionados a terceros de buena fe si el destinatario de los documentos firmados electrónicamente no comprueba ni tiene en cuenta las restricciones que figuren en el certificado en cuanto a sus posibles usos, o cuando no tenga en cuenta la suspensión o pérdida de vigencia del certificado publicada en la LCR, o cuando no verifique la firma electrónica.

14.8.2 Limitaciones de pérdidas

A excepción de lo establecido por las disposiciones de la presente DPC, la AC Raíz no asume ningún otro

compromiso ni brinda ninguna otra garantía, así como tampoco asumen ninguna otra responsabilidad ante suscriptores o terceros de buena fe.

14.9 Plazo y finalización

14.9.1 Plazo

Esta DPC estará en vigor mientras no se derogue expresamente por la emisión de una nueva versión o por la renovación de las claves de la AC Raíz, momento en que obligatoriamente se dictará una nueva versión.

14.9.2 Finalización

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

14.10 Notificaciones

Toda notificación, demanda, solicitud o cualquier otra comunicación requerida bajo las practicas escritas en esta DPC se realizará mediante documento o mensaje electrónico firmado digitalmente de conformidad con esta última o por escrito mediante correo certificado dirigido a cualquiera de las direcciones contenidas en el punto 6.5.2 persona contacto. Las comunicaciones electrónicas se harán efectivas una vez que las reciba el destinatario al que van

dirigidas.

14.11 Modificaciones

14.11.1 Procedimientos de especificación de cambios

La Autoridad con atribuciones para realizar y aprobar cambios sobre esta DPC es la Autoridad de Aprobación de Políticas (AAP).

14.11.2 Procedimientos de publicación y notificación

Toda modificación de esta DPC o de los Documentos de Política de Certificados se publicará en el sitio Web de SUSCERTE http://ww.suscerte.gob.ve

14.11.3 Procedimientos de aprobación de la Declaración de Prácticas de Certificación

El procedimiento para la aprobación de la declaración de prácticas de certificación es el resuelto por la Autoridad de Aprobación de Políticas. Asimismo compete a la AAP la aprobación y autorización de las modificaciones de dichos documentos.

14.12 Resolución de Conflictos

14.12.1 Resolución extrajudicial de conflictos

La AC Raíz podrá establecer, a través de los instrumentos jurídicos mediante los que se articule su relación con los PSC y verificadores, los procedimientos de mediación, arbitraje y resolución de conflictos que se consideren oportunos, todo ello sin perjuicio de la legislación de procedimiento administrativo.

14.12.2 Jurisdicción competente

Los conflictos que se plateen en la prestación por la AC Raíz de los servicios de certificación, se someterán a la jurisdicción, conforme a lo dispuesto en la LSMDFE y su Reglamento Parcial.

14.13 Legislación aplicable

El funcionamiento y operación de la AC Raíz, así como la presente DPC está regido por la legislación venezolana vigente en cada momento.

Explícitamente se asumen como de aplicación las siguientes leyes:

- Decreto 1.204 con Fuerza de Ley Sobre Mensajes de Datos y Firmas electrónicas (LSMDFE).
- Reglamento Parcial de la Ley Sobre Mensajes de Datos y Firmas Electrónicas LSMDFE).
- Ley Orgánica de Procedimientos Administrativos (LOPA).
- Ley Orgánica de Administración Pública (LOAP).

- Providencia administrativa de SUSCERTE Nº 016 Infraestructura Nacional de Certificación Electrónica.

14.14 Conformidad con la Ley aplicable

La AC Raíz declara que la presente DPC y PC cumple con las prescripciones contenidas en la LSMDFE. Adicionalmente es responsabilidad de la AAP velar por el cumplimiento de la legislación aplicable recogida en el apartado 14.13