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
3.3	Actualización General.	Noviembre 2012
3.4	Actualización General.	Julio 2013
4	Actualización General de acuerdo a las recomendaciones dadas para su adaptación a WebTrust.	Octubre 2014
4.1	Actualización General de acuerdo a las recomendaciones dadas por el auditor externo para su adaptación a la ETSI 102 042	Mayo 2015
4.2	Actualización de acuerdo a las observaciones de la Inspección y de la Auditoría del 2017	Diciembre 2017

ÍNDICE

TRÁMITE	
NOMBRE	**CARGO SUSCERTE**
Luis Prada Hector Poli Carlos Acosta	Superintendente Director de Servicios de Certificación Electrónica y Criptografía Director de Estandarización y Fiscalización de Certificación Electrónica y Seguridad de la información.
RESPONSABLE (S) DE LA EDICIÓN	
Nelly Pérez, Francis Ferrer	

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 acreditados, donde el certificado electrónico asocia la identidad de los mismos (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 electrónicamente como raíz, es decir posee un certificado autofirmado y es a partir de allí, donde comienza la cadena de confianza. Los campos del certificado raíz cumplen con los estándares internacionales y aplicables que garantizan la interoperabilidad.

La AC Raíz dispone de un certificado autofirmado con su clave privada, con el que firma los certificados de clave pública de los PSC acreditados, 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 CENDITEL Mérida, organismo adscrito al Ministerio para el Poder Popular para Educación Universitaria, Ciencia y Tecnología (MPPEUCT) y la Ley de Infogobierno.

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:

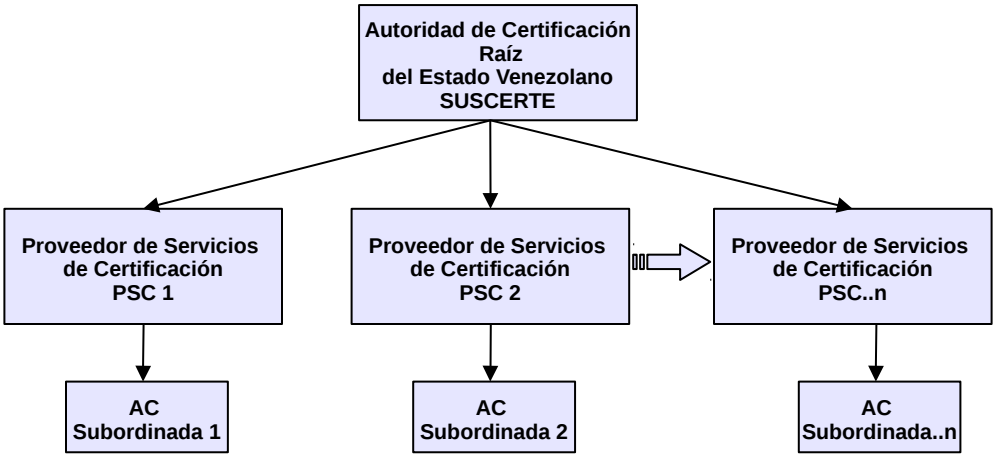

Figura Nº 1. *Arquitectura de la Infraestructura Nacional de Certificación Electrónica a nivel jerárquico*

La arquitectura jerárquica parte de la Raíz, ancla de la Cadena de Confianza de la Certificación Electrónica, llamada Autoridad de Certificación (AC) Raíz, desde la cual se inicia la Cadena de Confianza, una vez acreditado ante SUSCERTE según la Ley sobre Mensaje de Datos y Firma Electrónica (LSMDFE) se firma el certificado electrónico de los PSC, constituyendo el segundo nivel, además firma la Lista de Certificados Revocados (LCR) de la AC Raíz.

Los PSC emitirán los certificados electrónicos según los propósitos especificados en su propia DPC y PC, previa aprobación por parte de SUSCERTE.

En el tercer nivel se encuentran las AC Subordinadas de los PSC, 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 electrónicos de los PSC acreditados y Casos Especiales .

La Superintendencia de Servicios de Certificación Electrónica (SUSCERTE) está comprometida con proporcionar el nivel más alto de la seguridad, controles e integridad para apoyar nuestra Autoridad de Certificación llamada "Autoridad de Certificación Raíz del Estado Venezolano" de acuerdo con sus prácticas reveladas y descritas en esta Declaración de Prácticas de Certificación (DPC) y Políticas de Certificados (PC) diseñadas en cumplimiento de lo establecido en el estándar ETSI 102 042 versión 2.4.1. “Policy requeriments for certification authorities issuing public key certificate”.

SUSCERTE se ajusta a la versión actual de las Directrices del Foro CA/Browser Forum para emisión y gestión de certificados publicados en http://www.cabforum.org. En el caso de cualquier incompatibilidad entre este documento y estas Directrices, las mismas tienen prioridad sobre este documento. Además, la AC Raíz deberá incluir (directamente o por referencia) los requisitos aplicables de las Directrices en todos los contratos con las entidades emisoras subordinadas (Proveedores de Servicio de Certificación Electrónica (PSC) o Casos

Especiales), Autoridades de Registro y otros vinculados que impliquen o se relacionan con la emisión o mantenimiento de certificados electrónicos.

SUSCERTE, a partir del año 2014, ha sujeto sus prácticas de negocio de la Autoridad de Certificación Raíz, al nivel más alto de auditoría de acuerdo a la norma de WebTrust® para Autoridades de Certificación del AICPA/CICA y ETSI 102 042.

SUSCERTE opera los servicios de Autoridad de Certificación (AC) conocidos como "Autoridad de Certificación Raíz del Estado Venezolano", delegando en las Autoridades de Certificación Subordinadas denominadas "Proveedores de Servicios de Certificación" (PSC) y "Casos Especiales" (CE) las operaciones de certificación electrónica con las entidades finales, SUSCERTE proporciona los siguientes servicios de Autoridad de Certificación:

- Registro de Solicitud de Certificado de PSC y CE
- Emisión de certificado
- Distribución de certificado
- Renovación de certificado con cambio de clave
- Revocación y Suspensión de certificado y,
- Procesamiento de la lista de revocación de certificados (CRL)
- Comprobación de estado de certificados en línea (OCSP)

SUSCERTE es responsable de establecer y mantener controles eficaces sobre sus operaciones de AC, incluyendo la revelación de sus prácticas del negocio de la AC, integridad del servicio (incluyendo controles en la administración del ciclo de vida de la clave y el certificado), controles ambientales de la AC y control sobre los sistemas de seguridad de la red y de Certificados. Estos controles contienen

mecanismos de supervisión y se llevan a cabo acciones para corregir las deficiencias identificadas.

La AC raíz, los PSC y Casos Especiales debe desarrollar, implementar, hacer cumplir, publicar permanentemente en su sitio web, y actualizar periódicamente, según sea necesario sus propias y auditables Prácticas, políticas y procedimientos, en forma de Declaración de Prácticas de Certificación (CPS) y Política de Certificados (CP) que indican el cumplimiento de lo siguiente:

1. Poner en práctica los requisitos allí establecidos, y revisarlos anualmente;
2. Poner en práctica los requisitos del estándar WebTrust para CA vigente, el estándar WebTrust EV vigente o ETSI TS 102 042 V2.4.1; y
3. Toda la Infraestructura Nacional de Certificación Electrónica, desde la AC Raíz, los PSC, Casos Especiales y Autoridades de Tercer Nivel dependen de la prueba de la autenticidad de los Certificados EV.

Compromiso de cumplir las recomendaciones: El AC Raiz da fe de la validez de estas Directrices y todas las entidades adheridas a SUSCERTE deben incorporar estas directrices en sus respectivas políticas de EV, utilizando una cláusula como la siguiente : [Nombre del PSC o Caso Especial] se ajusta a la versión actual de las Directrices del Foro CA / Browser para la emisión y gestión de certificados de Validación Extendida publicados en http://www.cabforum.org. En el caso de cualquier incompatibilidad entre este documento y los Lineamientos, estas Directrices tienen prioridad sobre este documento.

2 REFERENCIAS NORMATIVAS

2.1 Constitución de la República Bolivariana de Venezuela.

2.2 Ley Orgánica de Procedimientos Administrativos (LOPA).

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

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

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

2.6 Ley de Infogobierno (Octubre 2013)

2.7 RFC 6960 Internet X.509 Public Key Infrastructure Online Certificate Status Protocol OCSP. 2013

2.8 RFC 5280 "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile". Mayo 2008

2.9 RFC 6818 "Updates to the Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile". Enero 2013

2.10 RFC 3647 “Internet x.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework”.

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

2.12 ETSI TS 102 042 “Policy requeriments for certification authorities issuing public key certificate”. 2.4.1.

2.13 ETSI TS 119 403 “Trust Service Provider Conformity Assessment – Requirements for conformity assessment bodies assessing Trust Service Providers”.

3 DEFINICIONES Y TERMINOLOGÍAS

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

AC RAÍZ	Primera autoridad en la jerarquía de la Infraestructura Nacional de Certificación Electrónica, operada y administrada por la Superintendencia de Servicios de Certificación Electrónica, quien se encarga del ciclo de vida de los certificados electrónicos a :

1) La propia Autoridad de Certificación RAÍZ del Estado Venezolano.
2) Las Autoridades de Certificación de los Proveedores de Servicios de Certificación Acreditados.
3) Las Autoridades de Certificación para casos especiales en proyecto de interés nacional.

AUTORIDAD DE CERTIFICACIÓN	Infraestructura tecnológica que se encarga de gestionar el ciclo de vida (emitir, renovar, revocar y suspender) de los certificados electrónicos.
AC PRINCIPAL DELPSC	Toda autoridad de certificación firmada por la AC RAÍZ, que proporciona certificados electrónicos a usuarios finales o AC Subordinada de un PSC.
AC SUBORDINADA DEL PSC	Toda autoridad de certificación que se encuentra firmada por una AC principal de un PSC, operada y administrada exclusivamente por este último, a los efectos de ampliar su esquema operativo o brindar mayores niveles de seguridad a su infraestructura tecnológica.
AUTORIDAD DE REGISTRO	Conjunto de infraestructura tecnológica y componente humano encargado de validar la identidad: así como, de verificar la veracidad y exactitud de los datos de identificación del solicitante de un certificado electrónico, y de la gestión operativa de las solicitudes relacionadas al ciclo de vida de un certificado electrónico.
AR EXTERNA	Entidad que bajo el control y supervisión del PSC acreditado realiza las funciones de AR dentro del proceso de expedición y manejo de los certificados electrónicos de forma exclusiva a una organización.

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.
PSC	Toda persona dedicada a proporcionar Certificados Electrónicos y demás actividades prevista en el Decreto Ley Sobre Mensajes de Datos y Firmas Electrónicas.
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.
SOLICITANTE	Persona aspirante a PSC y/o PSC acreditado que requiera:

	acreditación renovación, incorporar AC Subordinada y/o AR externas.
SOLICITUD	Requerimiento que realiza el solicitante para obtener una acreditación ante SUSCERTE, o efectúa un PSC acreditado para su renovación, incorporación de AC subordinada y/o AR externas.

4 SÍMBOLOS Y ABREVIATURAS

A los efectos de esta norma 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.
HSM	Módulo de Hardware Criptográfico.
ICP	Infraestructura de Clave Pública.
LCR	Lista de Certificados Revocados.
LOAP	Ley Orgánica de Administración Pública.
LOPA	Ley Orgánica de Procedimientos Administrativos.
LSMDFE	Ley Sobre Mensajes de Datos y Firmas Electrónicas.
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 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	**4.2**
Estado del documento	APROBADO
Referencia de la DPC/ OID (Object Identifier)	**DPC/PC AC Raíz/OID 2.16.862.1.1**
Fecha de emisión	**Julio 2006**
Fecha de expiración	La DPC y PC debe ser revisada con una periodicidad máxima de 2 años
Localización	Esta DPC y PC se encuentra en https://acraiz.suscerte.gob.ve

6 COMUNIDAD DE USUARIO Y APLICABILIDAD

6.1 Autoridad de Certificación (AC)

Es la entidad de confianza responsable de emitir, renovar, revocar y suspender los certificados electrónicos para los PSC, haciendo uso de la criptografía_de clave pública.

SUSCERTE se ajusta a la versión actual de las Directrices del Foro CA/Browser Forum para emisión y gestión de certificados publicados en http://www.cabforum.org. En el caso de cualquier incompatibilidad entre este documento y estas Directrices, las mismas tienen prioridad sobre este documento. Además, la AC Raíz deberá incluir (directamente o por referencia) los requisitos aplicables de las Directrices en todos los contratos con las entidades emisoras subordinadas (Proveedores de Servicio de Certificación Electrónica (PSC) o Casos Especiales), Autoridades de Registro y otros vinculados que impliquen o se relacionan con la emisión o mantenimiento de certificados electrónicos.

SUSCERTE, a partir del año 2014, ha sujeto sus prácticas de negocio de la Autoridad de Certificación Raíz, al nivel más alto de auditoría de acuerdo a la norma de WebTrust® para Autoridades de Certificación del AICPA/CICA y ETSI 102 042.

SUSCERTE opera los servicios de Autoridad de Certificación (AC) conocidos como "Autoridad de Certificación Raíz del Estado Venezolano", delegando en las Autoridades de Certificación Subordinadas denominadas "Proveedores de Servicios de Certificación" (PSC) y "Casos Especiales" (CE) las operaciones de certificación electrónica con las entidades finales, SUSCERTE proporciona los siguientes servicios de Autoridad de Certificación:

- Registro de Solicitud de Certificado de PSC y CE
- Emisión de certificado
- Distribución de certificado
- Renovación de certificado con cambio de clave
- Revocación y Suspensión de certificado y,
- Procesamiento de la lista de revocación de certificados (CRL)
- Comprobación de estado de certificados en línea (OCSP)

La estructura de los datos del certificado electrónico de la AC Raíz se presenta en la tabla Nº 1:

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 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	
country	VE	
emailAddress	acraiz@suscerte.gob.ve	
*telephoneNumber	<Teléfono de contacto>	
L	Caracas	
state	Distrito Capital	
PERÍODO DE VALIDEZ (VALIDITY)		
No antes de: (notBefore)	Fecha UTC en que el período de validez del certificado comienza	
No después de: (notAfter)	Fecha UTC 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 Certificacion Electronica	
country	VE	
emailAddress	acraiz@suscerte.gob.ve	
*telephoneNumber	<Teléfono de contacto>	
L	Caracas	
state	Distrito Capital	
INFORMACIÓN DE LA CLAVE PÚBLICA (SUBJECT PUBLIC KEY INFO)		
Algoritmo de clave pública (Public Key Algorithm)	RSAEncryption	
subjectPublicKey	modulus	4096 bit
	exponente	65537
EXTENSIONES		
Restricciones básicas (Basic Constraint)	Permite identificar si el signatario de un certificado es un certificador. Se debe definir como valor ***Crítico** * CA: True	
Nombre alternativo del emisor (Issuer Alternative Name)		
otherName	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	
keyIdentifier	Identificador de la clave pública de la AC Raíz	
authorityCertIssuer	<Contiene la información de la AC Raíz con el formato DN>	
*AuthorityCertSerialNumber	<Contiene el número del certificado del emisor>	
DirName	Contiene todos los datos del emisor	
authorityCertIssuer	<Contiene el número del certificado del emisor>	
Uso de claves (keyUsage)	Define el propósito de la clave del certificado. Se debe definir como valor ***Crítico**: Firma electrónica del certificado (**keyCertSign**) y firma de LCR (**cRLSign**)	
Nombre alternativo del titular (Subject Alternative Name)		
DNSName	suscerte.gob.ve	
Punto de distribución de LCR (distributionPoint)	Indica como se obtiene la información de LCR URI: https://www.suscerte.gob.ve/lcr	
	URI:https://acraiz.suscerte.gob.ve/lcr/	
	LDAP URI:ldaps://acraiz.suscerte.gob.ve/	
Acceso a la Autoridad de Información (Authority Info Access)	accessMethod	OCSP
	accessLocation	URI:https://ocsp.suscerte.gob.ve
	accessLocation	URI:http://acraiz.suscerte.gob.ve/ocsp/
	accessLocation	URI:https://acraiz.suscerte.gob.ve
	accessMethod	CAI
	accessLocation	<Dirección del Certificado de la Autoridad *.CRT>
Política de Certificados (PolicyInformation)	policyIdentifier	<OID asignado por SUSCERTE>
	cPSuri	(Lugar en internet desde donde se descargue la DPC y PC). URI:https://www.suscerte.gob.ve/

		dpc
	cPSuri	URI:https://acraiz.suscerte.gob.ve/dpc
Algoritmo de Firma (signatureAlgorithm)	Algoritmo actualizado	
Firma (signature)	<Contenido de la Firma>	

**** estos datos dependen de la migración del CE Raíz***

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

6.2 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 Proveedores de Servicios de Certificación y Casos Especiales

En el marco legal venezolano, los PSC acreditados y Casos Especiales 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 de la Infraestructura Nacional de Certificación Electrónica . Las AC de los PSC acreditados y Casos Especiales deben 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.

La estructura de los datos del certificado electrónico para los PSC acreditados 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 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	
country	VE	
emailAddress	acraiz@suscerte.gob.ve	
telephoneNumber	<Teléfono contacto>	
L	Caracas	
state	Distrito Capital	
PERÍODO DE VALIDEZ (VALIDITY)		
No antes de: (notBefore)	Fecha UTC en que el período de validez del certificado comienza	
No después de: (notAfter)	Fecha UTC en que el período de validez del certificado termina	
DATOS DEL TITULAR		
CN	<Identificación de la AC principal del Proveedor de Servicios de Certificación y/o Caso Especial>	
O	Sistema Nacional de Certificación Electrónica	
OU	<Nombre o razón social tal cual aparezca en el documento constitutivo>	
country	VE	
emailAddress	<correo electrónico de la AC del PSC)	
telephoneNumber	<Teléfono de contacto>	
L	(Dirección)	
state	(Estado)	
INFORMACIÓN DE LA CLAVE PÚBLICA (SUBJECT PUBLIC KEY INFO)		
Algoritmo de clave pública (Algorithm)	RSA Encryption	
Clave pública del titular	modulus	4096 bit

(subjectPublicKey)	exponent	65537
EXTENSIONES		
Restricciones básicas (Basic Constraint)	Permite identificar si el signatario de un certificado es un certificador. Debe ser **CRITICO** y contener el atributo CA. CA: True	
Nombre alternativo del emisor (Issuer Alternative Name)		
otherName	(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	
keyIdentifier	Identificador de la clave pública del AC Raíz	
authorityCertIssuer	Contiene la información de la AC Raíz con el formato DN	
authorityCertSerialNumber	Número de serie del certificado del emisor	
Define el propósito de la clave del certificado. Uso de claves (KeyUsage)	Firma de certificado	KeyCertSign(5)
	Firma LCR	cRLSign(6)
	Crítico	
Nombre alternativo del titular (Subject Alternative Name)		
DNS Name	(nombre de dominio del PSC y/o Casos Especiales registrado en nic.ve)	
Other Name	(Código de identificación del PSC acreditado y/o Casos Especiales asignado por SUSCERTE)	
otherName	(RIF del PSC y/o Casos Especiales)	
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) URI:https://acraiz.suscerte.gob.ve/lcr/CERTIFICADO-RAIZ-SHA384CRLDER.crl	
	URI:https://acraiz.suscerte.gob.ve	
	URI:ldaps://acraiz.suscerte.gob.ve	

Acceso a la Autoridad de Información (Authority Information Access)	accessMethod	[OCSP]
	accessLocation	(Enlace al servicio OCSP). URI:https://ocsp.suscerte.gob.ve
	accessLocation	URI:https://acraiz.suscerte.gob.ve/ocsp
Política de Certificados (PolicyInformation)	policyIdentifier	(OID autorizado por SUSCERTE)
	cPSuri	https://acraíz.suscerte.gob.ve/dpc

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

6.4 Estructura de los datos del certificado de Servidor del publicador de la AC RAÍZ

La estructura de los datos del certificado de servidor del publicador de la AC Raíz se presenta en la tabla N° 3

CAMPO DEL CERTIFICADO	Valor del Certificado de la AC principal del PSC
Versión	V3
Serial	Identificador único del certificado. No mayor de 20 Octetos.
Algoritmo de firma	Debe contener el OID del algoritmo y de ser necesarios, los parámetros asociados usados por el certificador. Los algoritmos permitidos son SHA256 y SHA384 with RSAEncryption.
DATOS DEL EMISOR	
CN	Autoridad de Certificación Raíz del Estado Venezolano
O	Sistema Nacional de Certificación Electrónica
OU	Superintendencia de Servicios de Certificación Electrónica
country	VE
TelephoneNumber	(Teléfono de contacto de la AC Raíz)

emailAddress	acraiz@suscerte.gob.ve	
L	Caracas	
state	Distrito Capital	
PERÍODO DE VALIDEZ (VALIDITY)		
Período de Validez	Este período de validez del certificado de servidor no debe de exceder a 1 año	
DATOS DEL TITULAR		
CN	Nombre que identifica al Dominio o Subdominio del servidor (acraiz.suscerte.gob.ve)	
Serial Number	G-20004036-0	
organization	Superintendencia de Servicios de Certificación Electrónica	
BusinessCategory (necesario para certificados EV)	Government Entity	
JurisdictionCountryName (necesario para certificados EV)	VE	
postalCode	1020	
OU	Dirección de Servicios de Certificación Electrónica y Criptografía	
country	VE	
emailAddress	acraiz@suscerte.gob.ve	
telephoneNumber	(número telefónico de contacto de la AC Raíz, opcional)	
locality	Caracas	
streetAddress	Avenida Universidad	
state	Distrito Capital	
INFORMACIÓN DE LA CLAVE PÚBLICA (SUBJECT PUBLIC KEY INFO)		
Algoritmo de clave pública (Public Key Algorithm)	RSA Encryption	
Tamaño de clave pública	modulus	2048bit
	exponent	65537
EXTENSIONES		
Restricciones básicas (Basic Constraint)	Critico, CA: False	
Usos Permitidos para el certificado electrónico (KeyUsage)		
Digital Signature	0	

Content Commitment	1	
Key Encipherment	2	
Data Encipherment	1	
KeyAgreement	**2**	
Uso Mejorado o extendido permitido para el certificado electrónico (Extended Key Usage)		
ServerAuth	1.3.6.1.5.5.7.3.1	
Identificador de clave de Autoridad Certificadora (Authority Key Identifier)		
Keyidentifier	Identificador de la clave pública de la AC Raíz	
AuthorityCertIssuer	Contiene el DN de la AC Raíz	
authorityCertSerialNumber	Número del certificado de la AC Raíz	
Identificador de clave del titular (Subject Key Identifier)	Valor hexadecimal del identificador de la clave (hash)	
Nombre alternativo del titular (Subject Alternative Name)		
OtherName	G-20004036-0	
rfc822Name	(correo contacto de la AC Raíz)	
DNS	DNS primario	
DNS	DNS secundario	
Nombre alternativo del emisor (Issuer Alternative Name)		
DNSName	(DNS del emisor del certificado)	
OtherName	(RIF del PSC)	
OtherName	(codigo de identificación del PSC)	
Puntos de Distribuición de LCR (CRL Distribution Point)	(LCR del repositorio del PSC)	
Acceso a la Autoridad de Información (Authority Information Access)	accessMethod	(OCSP)
	accesslocation	(URL del servicio OCSP del PSC)
Política de Certificados (PolicyInformation	policyidentifier	(OID autorizado por SUSCERTE)
	CPSuri	(dirección donde se puede descargar la PC
	userNotice	(Certificado de Servidor, v1.0)
signatureAlgorithm	Algoritmo autorizado	

signature	(contenido de la firma)

Tabla Nº 3. *Estructura de los datos del certificado de Servidor*

6.5 Tercero de Buena Fe

Entidad que confía en los datos contenido en un certificado electrónico.

7 USO DE LOS CERTIFICADOS

7.1 Uso permitido para los certificados

El certificado electrónico raíz sólo puede utilizarse para la identificación de la propia AC Raíz.

El uso de los certificados emitidos por la AC Raíz estará limitado a la firma de certificados electrónicos de los PSC y Casos Especiales, para el servicio de verificación en línea del estatus del certificado (OCSP) y las listas de certificados revocados (LCR).

7.2 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.

8 POLÍTICAS DE ADMINISTRACIÓN DE LA AC RAÍZ

8.1 Especificaciones de la Organización Administrativa

Nombre	Superintendencia de Servicios de Certificación Electrónica.
Correo electrónico	acraiz@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	https://acraiz.suscerte.gob.ve

8.2 Persona Contacto

Nombre	Superintendencia de Servicios de Certificación Electrónica.
Correo electrónico	acraiz@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	https://acraiz.suscerte.gob.ve

8.3 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.

La AAP está conformada por personal de la Dirección de Servicios de Certificación Electrónica y Criptografía (DSCEC) y la Dirección de Estandarización y Fiscalización en Certificación Electrónica y Seguridad de la Información (DEF).

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

9.1 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: https://acraiz.suscerte.gob.ve/

  Sección: Certificados

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

  web: https://acraiz.suscerte.gob.ve/lcr/CERTIFICADOS-RAIZ-SHA384CRLDER.crl

  Sección: Lista de Certificados Revocados

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

- **Para la DPC:**

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

  Sección: Declaración de Prácticas de Certificación

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

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

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

9.2 Publicación

Es obligación para la AC Raíz, Casos Especiales y los PSC acreditados pertenecientes a la jerarquía de la Infraestructura Nacional de Certificación Electrónica publicar la información relativa a sus DPC y PC, 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: https://acraiz.suscerte.gob.ve/dpc en formato PDF.
- El certificado de la AC Raíz y los emitidos por ésta, se encuentran disponibles en el repositorio público, en formato X.509 v3 y en la dirección https://acraiz.suscerte.gob.ve. Sección: certificados.
- Los datos de contacto de SUSCERTE se encuentran en la dirección https://acraiz.suscerte.gob.ve

9.3 Frecuencia de Publicación

9.3.1 Certificados de la AC Raíz

La publicación del certificado electrónico de la Ac raíz se realizará con anterioridad a su puesta en vigencia a través de la Gaceta Oficial. El período de validez es de hasta veinte (20) años.

9.3.2 Certificados del PSC acreditados

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

9.3.3 Lista de Certificados Revocados (LCR)

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

- **Periódicamente**:

  Cada seis (6) meses.

- **Eventualmente:**

  Cada vez que se acredite o revoque un certificado dentro de la Infraestructura Nacional de Certificación Electrónica. Cuando suceda uno de estos eventos, el período de seis (6) meses es reiniciado.

9.3.4 Declaración de Prácticas de Certificación

La AC Raíz, publica en el repositorio, las nuevas versiones de este documento, en un lapso máximo de cinco (5) días hábiles luego de su aprobación.

9.3.5 Casos Especiales

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

9.3.6 Servicio de Validación en línea (OCSP)

El servicio de validación en línea (OCSP) es actualizado cada seis (6) meses.

9.4 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.

10 IDENTIFICACIÓN Y AUTENTICACIÓN

10.1 Registros de Nombres

10.1.1 Tipos de Nombres

La AC Raíz, sólo genera y firma certificados con tipos de nombres acordes al estándar X. 509 versión 3.

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

- CN = Autoridad de Certificacion Raíz del Estado Venezolano
- O = Sistema Nacional de Certificación Electrónica
- 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 Certificación y/o Casos Especiales]
- O = Sistema Nacional de Certificación Electrónica
- 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 dos 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.

El Identificador único de Objeto (OID) de la DPC y la PC, bajo ninguna circunstancia debe ser modificada.

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 .

10.1.2 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.

10.1.3 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.

10.1.4 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.

10.1.5 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.

10.2 Validación inicial de la identidad

10.2.1 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.

10.2.2 Autenticación de la identidad de una organización

El PSC y/o Casos Especiales deben presentar la solicitud de acreditación y/o renovación ante SUSCERTE en conjunto de una serie de recaudos de carácter legal, económico-financiero y técnico, a objeto de validar la suficiencia de la capacidad económica-financiera y técnica y garantizar que estén legalmente constituidos, así como la verificación de la identidad. Así mismo esta verificación se lleva a cabo de forma anual, a través de los procesos de renovación de la acreditación. Los

recaudos son los siguientes:

- Nombre completo de la unidad organizativa
- Dirección física de funcionamiento u otra características mediante las cuales describen como puede ser contactado el PSC o Casos Especiales
- Cédula de Identidad o Pasaporte de los representantes legales.
- Registro de Información Fiscal (RIF).
- Actas constitutivas y Estatutos sociales, actas de asambleas ordinarias y/o extraordinarias, celebradas por el solicitante en caso de persona de derecho privado.
- Gaceta Oficial de la publicación del decreto de creación, Gaceta Oficial donde conste el nombramiento o las atribuciones del o los representantes legales, o documento en el que conste la capacidad para actuar en nombre y representación del solicitante, en caso de persona de derecho público.
- 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 o Renovación de Proveedores de Servicio de Certificación y para la Incorporación de AC Subordinadas y/o AR Externas”, 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 N° 10 de SUSCERTE denominada “Manual de Acreditación y Rrenovación de Proveedores de Servicios de Certificación”.

Dichas normas, cuando sean de carácter público, se encuentran disponible en el sitio web https://www.suscerte.gob.ve/ en la sección de Biblioteca específicamente en el enlace llamado: Normativa.

10.2.3 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.

10.2.4 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 las legislaciones aplicables. Garantizando así los requisitos de seguridad, validez y vigencia del certificado.

10.3 Identificación y autenticación de solicitudes de renovación de claves

10.3.1 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 (Validación inicial de la identidad). Este método de renovación requiere que la clave privada no este ni vencida ni revocada.

10.3.2 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 (Validación inicial de la identidad). 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.

10.4 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, y el subscriptor, debidamente identificado, debe demostrar y sustentar las causas y motivos de la revocación.

La política de autenticación acepta solicitudes de revocación firmadas de forma manual en las instalaciones de SUSCERTE, por el representante legal del subscriptor del certificado, a objeto de verificar la pertinencia legal de la misma.

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.

También se podrá revocar la clave en caso de cese de actividades y en caso de incumplimiento de algunas de las obligaciones previstas en la Ley y en el reglamento, lo cual ameritará la revocación de la acreditación.

En todo caso la solicitud de revocación no podrá excederse de 24 horas a partir de la comprobación de la pertinencia legal de la misma.

11. EL CICLO DE VIDA DEL CERTIFICADO DE LA AC RAÍZ

11.1 Procesos de firma del certificado de la AC Raíz

11.1.1 Procedimiento para generación del certificado de la AC RAÍZ

La Autoridad de Certificación Raíz del Estado Venezolano es creada a partir del Decreto con Fuerza de Ley N° 1204, que establece una arquitectura jerárquica para la Cadena de Confianza donde no existe otra AC que pueda firmar el certificado de la AC Raíz, siendo éste el único caso en el que se genera un certificado electrónico autofirmado.

La firma del certificado es realizada siguiendo el procedimiento técnico estipulado en el Manual de Operación de la AC Raíz, en ceremonia pública con la presencia de un tercero de confianza que avale el procedimiento, cumpliendo con las notificaciones legales pertinentes.

11.1.2 Publicación del certificado de la AC RAÍZ

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 generación del certificado.

11.2 Proceso de renovación del certificado de la AC RAÍZ

11.2.1 Causa para la renovación del certificado de la AC RAÍZ

La causa de la renovación del certificado de la AC Raíz del Estado Venezolano, es por la caducidad.

11.2.2 Procedimiento para la renovación del certificado de la AC RAÍZ

Máximo tres (3) años previos a la caducidad del certificado de la AC Raíz vigente, se generará un nuevo par de claves y certificado electrónico de AC Raíz con una vigencia de 20 años, con la cuál se firmarán los certificados electrónicos de los PSC.

SUSCERTE deberá notificar a los PSC sobre la proximidad del vencimiento de la AC Raíz y de sus propios certificados, informando además sobre el momento de generación del nuevo par de claves y del certificado electrónico de la AC Raíz, notificando que deben enviar la solicitud de renovación de certificado electrónico. Es importante destacar que durante el proceso de renovación de la AC Raíz, se generarán los nuevos certificados de los PSC bajo la nueva AC Raíz y en ese sentido, se efectuará una ceremonia pública, siguiendo el proceso de creación y firma de la AC Raíz, que debe cumplir con las notificaciones legales pertinentes.

Adicionalmente, se deberá actualizar la huella del nuevo certificado electrónico de la AC Raíz en la DPC.

11.2.3 Publicación del certificado renovado de la AC RAÍZ

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 del certificado.

11.3 Proceso de revocación del certificado de la AC RAÍZ

11.3.1 Circunstancias para la revocación del certificado de la AC RAÍZ

Las circunstancias para la revocación del certificado de la AC Raíz son las siguientes:

- Compromiso de la clave privada de la AC Raíz.
- Por resolución judicial o administrativa que lo ordene.

11.3.2 Procedimiento para la revocación del certificado de la AC RAÍZ

Una vez revocado el certificado de la AC Raíz, se deberá efectuar un borrado seguro de todas las instancias y respaldos de la clave privada de la AC Raíz.

Los pasos para la revocación del certificado electrónico de la AC Raíz, son los siguientes:

RESPONSABLE	ACCIÓN
SUPERINTENDENTE	Notifica al representante legal de los PSC sobre la revocación del certificado electrónico de la AC Raíz y pública la medida a través de las vías pertinentes.
DIRECTOR(A) DSCEC	El Director(a) convoca a los poseedores de las tarjetas de operador de resguardo de la clave privada de la AC Raíz y solicita al operador(a) de la AC que inicie el proceso de revocación del certificado de la AC Raíz.
OPERADOR(A) AC	Inicia el Sistema de gestión de la AC Raíz, revoca los certificados emitidos por la AC y genera una LCR donde se revoque la AC Raíz, con un tiempo de duración igual al tiempo de vigencia que le reste a la AC Raíz.
DIRECTOR(A) DSCEC	Solicitará a los PSC acreditados que emitan una solicitud de certificado electrónico para la emisión de un nuevo certificado.
OPERADOR(A) AC	Efectúa el procedimiento de generación de un nuevo par de claves para la AC Raíz y emite un nuevo certificado electrónico autofirmado.
PSC	Genera una solicitud de certificado electrónico (CSR). Hace acto de presencia en la ceremonia de generación del nuevo

	certificado electrónico.
OPERADOR(A) AC	Emite el certificado electrónico del PSC bajo la nueva AC Raíz,reestableciendo la infraestructura PKI. Actualiza los publicadores de la AC Raíz.
DIRECTOR(A) DSCEC	Actualiza la DPC para la inclusión de la huella del nuevo Certificado Electrónico.

Todo este procedimiento debe realizarse en presencia de un notario público

11.3.3 Publicación del nuevo certificado de la AC Raíz

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 generación del certificado.

12. EL CICLO DE VIDA DE LOS CERTIFICADOS PARA PSC Y CASOS SPECIALES

12.1 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 https://acraiz.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.

12.1.1 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.

12.1.2 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 (https://www.suscerte.gob.ve) o en sus oficinas, los requisitos para su trámite
AUDITOR ACREDITADO	2. Efectúa la auditoría respectiva, emitiendo informe. 3. Envía informe de auditoría al solicitante.
SOLICITANTE	4. Recibe informe de auditoría. 5. Si el informe de auditoría refleja no conformidades. a. Debe subsanar las no conformidades. b. Contactar al auditor para informar la remediación.
AUDITOR ACREDITADO	6. Debe dar fe de la remediación del solicitante, dejando constancia en su informe definitivo.
SOLICITANTE	7. Deposita en la entidad bancaria indicada por SUSCERTE, la tasa correspondiente para la acreditación o renovación, si aplica. 8. Entrega planilla de solicitud llena, comprobante de déposito y recaudos, en caso de renovación deben consignarse 45 días contínuos antes del vencimiento de la acreditación.

SUSCERTE	9. Recibe solicitud, pago y recaudos clasificados 10. Verifica que los recaudos estén completos a) Si los recaudos están completos i) Admite solicitud de acreditación ii) Envía notificación al solicitante b) Si faltan recaudos: i) Se indica al solicitante recaudo faltante 11. Queda a criterio de la máxima autoridad de la Superintendencia solicitar se lleven a cabo inspecciones técnicas a las instalaciones del Solicitante, cuyo resultado se tomará en cuenta para la aprobación del trámite. 12. Evalúa si el solicitante cumple todos los requisitos exigidos a) Si cumple los requisitos: i) El trámite solicitado es aprobado ii) Envía notificación de aprobación al solicitante b) Si no cumple los requisitos: i) El trámite solicitado resulta negado ii) Envía notificación al solicitante iii) Ir al paso 19.
SOLICITANTE	13. Recibe notificación de aprobación 14. Si corresponde, tramita y presenta las garantías que le exige la LSMDFE y su Reglamento Parcial, de conformidad con lo establecido por SUSCERTE (Ver apartado 2.2.7 de la norma 27).
SUSCERTE	15. Recibe las garantías constituidas a) Si las garantías corresponden con los elementos requeridos por SUSCERTE: i) Ir al paso 16 b) Si las grantías no corresponden con los elementos requeridos por SUSCERTE: i) Se niega la solicitud ii) Finaliza el proceso 16. Emite Providencia Adminsitrativa contentiva de la acreditación o renovación del solicitante, publicándola en la Gaceta Oficial de la República Bolivariana de Venezuela 17. En caso de careditación se emite Certificado a la AC Principal del PSC

	18. Finaliza el proceso
SOLICITANTE	19. Recibe notificación de negación 20. Decide su actuación respecto a respuesta de SUSCERTE. a) Si esta de acuerdo. i) Finaliza el proceso b) Si no esta de acuerdo. i) Puede ejercer los recursos legales correspondientes. ii) Finaliza el proceso.

12.2 Tramitación de solicitud de un certificado

12.2.1 Realización de las funciones de identificación y autenticación

Las funciones de identificación y autenticación son realizadas por el personal de SUSCERTE que labora en cada área de acuerdo a la competencia de los recaudos consignados por el solicitante; a tales efectos, se llevará un registro de las observaciones realizadas de carácter Técnico, Legal y Económico-Financiero.

12.2.2 Aprobación o denegación de certificado

Se aprobará las solicitudes de certificación a aquellos PSC 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 .

12.2.3 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 en conjunto con todos los requisitos.

12.3 Emisión de Certificado

Luego de verificar y aprobar las exigencias establecidas en la LSMDFE el sistema de la AC Raíz procederá a realizar la emisión del certificado al PSC y/o Casos Especiales mediante la publicación en la Gaceta Oficial de la República Bolivariana de Venezuela.

12.3.1 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 período de validez se inicie en el futuro o una fecha posterior a la actual.

12.3.2 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 Gaceta Oficial, la autorización para que el solicitante comience a actuar como PSC.

12.4 Aceptación de Certificados

12.4.1 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 .

12.4.2 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.

12.4.3 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.

12.5 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.

12.5.1 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 de la AC principal de los PSC y Caso Especiales, firma de LCR y del certificado del servicio OCSP.

12.5.2 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.

12.6 Renovación de certificado con cambio de clave

12.6.1 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.

12.6.2 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

12.6.3 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 12.1.

Como única diferencia, para garantizar la no existencia de dos certificados válidos al mismo tiempo para un mismo PSC bajo una misma PC, deben revocarse todos certificados existentes antes de proceder a realizar la renovación.

12.6.4 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 Gaceta Oficial.

12.6.5 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.

12.6.6 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.

12.7 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.

12.8 Revocación y suspensión de un certificado

Una vez revocado el certificado de la Autoridad de Certificación, el PSC deberá efectuar un borrado seguro de todas las instancias y respaldos de la clave privada de la AC y de sus AC Subordinadas.

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

Un certificado del PSC y/o Casos Especiales se revocará dentro de los siete (7) días si uno o mas de la circunstancias siguientes ocurren:

- 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 revocación de su certificado por escrito.
- Por resolución judicial o administrativa que lo ordene.
- Por la variación de los datos del certificado.
- Por revocación de la acreditación.
- Por Cese de operaciones.
- Cuando el PSC y/o Casos Especiales no cumple con los requisitos de su PC y DPC.
- Cuando la revocación es requerida en su PC y DPC.

- Cuando la AC Raíz obtiene prueba de que el certificado es mal utilizado.
- Cuando el contenido técnico presenta riesgo inaceptable para el software de aplicación (criptografía y algoritmo de firma obsoletos, por lo tanto los certificados deben ser derogados y sustituidos en una AC en un plazo determinado).

12.8.2 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

12.8.3 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

12.8.4 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 donde se pueda anular la solicitud de revocación.

12.8.5 Circunstancias para la suspensión

La Autoridad de Certificación Raíz del Estado Venezolano no prevé procedimientos para la suspensión de certificados electrónicos.

12.8.6 Entidad que puede solicitar la suspensión

La Autoridad de Certificación Raíz del Estado Venezolano no prevé

procedimientos para la suspensión de certificados electrónicos.

12.8.7 Procedimiento para la solicitud de suspensión

La Autoridad de Certificación Raíz del Estado Venezolano no prevé procedimientos para la suspensión de certificados electrónicos.

12.8.8 Límites del período de suspensión

La Autoridad de Certificación Raíz del Estado Venezolano no prevé procedimientos para la suspensión de certificados electrónicos.

12.8.9 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 debe estar disponible 24 horas al día, 7 días a la semana, y los 365 días del año.

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 seis (6) meses o cada vez que se acredite o revoque un certificado dentro de la Infraestructura Nacional de Certificación Electrónica. Cuando suceda uno de estos eventos, el período es reiniciado.

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.

10.8.10 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: https://acraiz.suscerte.gob.ve/

12.8.11 Disponibilidad de comprobación on-line de revocación

La AC Raíz posee un servidor OCSP para la verificación online del estado de los certificados. El repositorio en donde se puede realizar la comprobación en línea esta descrita en el apartado 9.1

12.8.12 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.

12.8.13 Otras formas de divulgación de información de revocación disponibles

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

12.9 Servicios de comprobación de estado de certificados

12.9.1 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 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.

12.9.2 Disponibilidad del Servicio

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

12.9.3 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.

12.10 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 12.8.1.
- Caducidad de la vigencia del certificado. En el apartado 12.8.3 de la DPC se detalla el procedimiento para la solicitud de la revocación.

12.11 Custodia y recuperación de la clave

12.11.1 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 límite (k,n) de Shamir tanto en software como en dispositivos criptográficos, lo que permite establecer una custodia compartida de la clave privada entre varios responsables.

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

13.1 Controles de Seguridad Física

13.1.1 Ubicación y construcción

Las operaciones críticas de la AC Raíz están protegidas físicamente con medidas de seguridad diseñadas de acuerdo a la criticidad de sus elementos 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.

13.1.2 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.

13.1.3 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 ininterrumpida (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.

13.1.4 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.

13.1.5 Protección y prevención de incendios

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

13.1.6 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.

13.1.7 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.

13.1.8 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.

13.2 Controles Funcionales

13.2.1 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:

- Custodios de la AC Raíz.
- Operador de la AC Raíz.
- Oficial de Seguridad de la Información.
- Auditor Interno.
- Coordinador de la Autoridad de Certificación.

13.2.2 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

13.2.3 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.

13.3 Controles de Seguridad Personal

13.3.1 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.

13.3.2 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 Infraestuctura de Clave Pública (ICP).
- Declaración de Prácticas de Certificación y las Política de certificados pertinentes.

- Gestión de los tipos de incidentes que son probables de ocurrir.

13.3.3 Requerimientos y frecuencia de actualización de la formación

SUSCERTE, preveera formación o capacitación 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.

13.3.4 Frecuencia y secuencia de rotación de roles

No aplica este apartado

13.3.5 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.

13.3.6 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
- Plan de Contingencia
- Política de certificados
- Política de Seguridad de la Información
- Organigrama y funciones del personal

13.4 Procedimiento de Control de Seguridad

13.4.1 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.

13.4.2 Frecuencia de procesado de registros de logs

Los registros de logs se analizan con una frecuencia mensual o cuando hay eventos extraordinarios. Cada extracción de logs también deja

trazas de auditorías para su posterior revisión.

13.4.3 Periodo de retención para los logs de auditoría

La AC Raíz retendrá todos los registros de auditoría generados por el sistema por un periodo mínimo desde la fecha de su creación de diez (10) años para las auditoría mensuales.

13.4.4 Protección de los logs de auditoría

La integridad de los logs 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, en las instalaciones seguras de la AC Raíz.

13.4.5 Procedimientos de respaldos de los logs de auditoría

Se generan copias de seguridad incrementales, de acuerdo con la Política de Copias de Seguridad.

Las copias de respaldos de los logs de auditoría de la AC Raíz se almacenan en archivos seguros ignífugos.

13.4.6 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.

13.4.7 Notificación al sujeto causa del evento

No aplica este apartado.

13.4.8 Análisis de seguridad

Se establece la realización de, al menos, un análisis anual de seguridad sobre los componentes de la plataforma de la AC Raíz. Es responsabilidad de la AC Raíz coordinar dichos análisis a través del Oficial de Seguridad. Es responsabilidad de la AC Raíz informar a los equipos auditores de la suspensión de los análisis.

Los análisis de seguridad implican el inicio de las tareas precisas para detectar y/o corregir las vulnerabilidades detectadas, así como la emisión de un contra-informe por parte de la AC Raíz.

13.5 Archivo de Informaciones y Registros

13.5.1 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.

13.5.2 Período de retención para el archivo

Las trazas de los archivos son conservadas durante un período de diez (10) años.

13.5.3 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.

13.5.4 Procedimientos de backup del archivo

Este apartado no aplica.

13.5.5 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.

13.5.6 Sistema de repositorio de archivos de auditoría (interno vs externo)

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

13.5.7 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, el tiempo de su generación y se crea una incidencia en el caso de errores o comportamientos imprevistos.

Mediante inspecciones se verificará el período de hasta diez (10) años que deben permanecer almacenados los archivos de respaldos y retención de los logs en general, una vez destruidas las claves de la AC Raíz.

13.6 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.

13.7 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 SUSCERTE 052 , son los siguientes:

13.7.1 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.

13.7.2 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).

13.7.3 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.

13.7.4 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.

13.8 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.

14. CONTROLES DE SEGURIDAD TÉCNICA

14.1 Generación e instalación de par de claves

14.1.1 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.

14.1.2 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.

14.1.3 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.

14.1.4 Disponibilidad de la clave pública

La clave publica de la AC Raíz y su fingerprint (***huella digital. Ver Anexo N° 1***.) estará disponible en https://acraiz.suscerte.gob.ve las 24 horas del día los 7 días de la semana y los 365 días al año de forma continua.

14.1.5 Tamaño de las claves

Los algoritmos criptográficos empleados por la AC Raíz para firmar los certificados y las LCR son , SHA256withRSA y SHA384withRSA. La longitud de la clave con el algoritmo RSA de la AC Raíz y del PSC es de 4096 bits.

14.1.6 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

14.1.7 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 3 de 9 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.

14.1.8 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

14.2 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 la confidencialidad de la clave privada, de la misma forma en que se resguarda la clave privada original.

14.2.1 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.

14.2.2 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.

14.2.3 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.

14.2.4 Copia de seguridad de la clave privada

Las copias de seguridad de las claves privadas de componentes de la AC Raíz se almacenan en archivos seguros ignífugos.

14.2.5 Archivo de la clave privada

Las copias de seguridad de las claves privadas se almacenan en custodia cifradas en archivos seguros ignífugos por un período de ***hasta*** 10 años, los cuales son verificados a través de las inspecciones

de la retención de logs y respaldo en general, garantizando los períodos de retención.

14.2.6 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.

14.2.7 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 tres (3) de nueve (9) operadores de resguardo de la clave privada con sus respectivas tarjetas de operador, de las cuales tres (3) tarjetas se encuentran en el centro alterno y las otras seis (6) en el centro principal.

14.2.8 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

14.2.9 Método de destrucción de la clave privada

La AC Raíz eliminará su clave privada; la instancia del centro de datos principal, la instancia del centro de datos alterno y las instancias existentes en las copias de respaldo, 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.

No se contempla la destrucción de HSM, debido a su alto coste. En su lugar se procederá a las tareas de borrado seguro de las claves en él contenidas.

La destrucción del Token de las tarjetas criptográficas puede realizarse cuando la información impresa en la misma pierda validez y deba emitirse una nueva tarjeta.

La tarea a realizar consiste en una Destrucción Segura del Token a nivel físico.

En caso de revocación de la clave privada la destrucción de los respaldos serán efectuado mediante un borrado seguro.

14.2.10 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.

14.3 Otros aspectos de la gestión del par de claves

14.3.1 Archivo de la clave pública

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

14.3.2 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 ***hasta*** veinte (20) años, mientras que el de los PSC tendrá una validez de ***hasta*** diez (10) años y el de los Casos Especiales por ***hasta*** un (01) año. Por otro lado los períodos de operación de los certificados serán de la mitad del período de validez.

14.4 Datos de activación

14.4.1 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.

14.4.2 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.

14.5 Controles de seguridad del computador

14.5.1 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.

14.5.2 Calificaciones de seguridad computacional

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

14.6 Controles de seguridad del ciclo de vida

14.6.1 Controles de desarrollo de sistemas

No aplica este apartado

14.6.2 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.

14.6.3 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.

14.7 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.

14.8 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.

15 PERFILES DE CERTIFICADOS, LCR Y OCSP

15.1 Perfil del certificado

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

- 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).
- RFC 5280 "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile". Mayo 2008
- RFC 6818 "Updates to the Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile". Enero 2013

15.1.1 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.

15.1.2 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
- SubjectAlternativeName. Marcada como crítica
- LCRDistributionPoint. Marcada como crítica

15.1.3 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)

15.1.4 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).

15.1.5 Restricciones de los nombres

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

15.1.6 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

Los OID'S correspondiente tanto a la DPC como a las PC de la AC Raíz, bajo ninguna circunstancia deben ser modificados.

15.1.7 Uso de la extensión "Policy Constraints"

No se estipula su uso.

15.1.8. Sintaxis y semántica de los cualificadores de política

No se estipula su uso.

15.1.9. Tratamiento semántico para la extensión critica "Certificate Policy"

La extensión "Certificate Policy" identifica la política que define las practicas que la AC Raíz asocia explícitamente con el certificado. Adicionalmente la extensión puede contener un cualificador de la política.

15.2 Perfil de la LCR

15.2.1 Número de versión

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

15.2.2 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

15.3 Perfil de OCSP

15.3.1 Número de versión

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

15.3.2 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

15.3.3 Perfil de certificado de servicio de OCSP

La estructura de los datos del certificado de servicio de OCSP se presenta en la tabla N° 4.

Campo del Certificado	Valor del Certificado
Versión	V3
Serial	Identificador único del certificado. Este número se asigna de forma consecutiva.
Algoritmo de Firma	Debe contener el OID del algoritmo y de ser necesarios, los parámetros asociados usados por el certificador. El algoritmo permitido es SHA256 con cifrado RSA.
Datos del Emisor (DN)	
CN	Autoridad de Certificación Raíz del Estado Venezolano
O	Sistema Nacional de Certificación Electrónica
OU	Superintendencia de Servicios de Certificación Electrónica
C	VE
E	acraiz@suscerte.gob.ve
L	Caracas
ST	Distrito Capital
Período de Validez (Validity)	

No antes de: (no before)	Fecha en que el período de validez del certificado comienza
No después de: (No After)	Fecha en que el período de validez del certificado termina (menor o igual a 1 año)
Datos del Titular	
CN	OCSP Responder de la AC Raíz del Estado Venezolano
O	Sistema Nacional de Certificación Electrónica
OU	Dirección de Certificación Electrónica y Criptografía
C	VE
E	acraiz@suscerte.gob.ve
L	Caracas
ST	Distrito Capital
Información de la Clave Pública (Subject Public Key info)	
Algoritmo de clave pública (Public Key Algorithm)	RSAEncryption
Tamaño de clave pública	2048
Extensiones	
Restricciones básicas (Basic Constraint)	CA: False y pathLenConstraint = 0
Usos permitidos para el certificado electrónico (Key Usage)	
Digital Signature	1
No Repudiation	1
Uso mejorado o extendido permitido para el certificado electrónico (Extended Key Usage)	
ocspSigning	1.3.6.1.5.5.7.3.9
ocspNocheck	1.3.6.1.5.5.7.48.1.5
Identificador de clave de Autoridad Certificadora (Authority Key Identifier).	
Keyid	Valor hexadecimal (Identificador de la clave pública)
DirName	Contiene el DN (C, O, OU, ST, L, CN, E) de la AC Raiz
Serial Number	Número positivo (Contiene el número del certificado del emisor)
Identificador de clave del titular (Subject Key Identifier).	Campo para identificar el certificado que contienen una clave pública particular.
Nombre Alternativo del Titular (Subject Alternative Name)	
DNSname	https://www.suscerte.gob.ve
OtherName	OID 2.16

	.862.2.1
OtherName	G-20004036-0
Nombre Alternativo del Emisor (Issuer Alternative Name)	
DNSname	Nombre DNS del PSC
OtherName	OID 2.16.862.2.2
Acceso a la Autoridad de Información (Authority Information Access)	URI:https://ocsp.suscerte.gob.ve
Política de Certificados (Certificate Policies)	CPS:https://www.suscerte.gob.ve/dpc Policy: 2.16.862.3.1.2

Tabla Nº 4 *Perfil de certificado de servicio de OCSP*

16 AUDITORÍA DE CONFORMIDAD

16.1 Frecuencia de los controles de conformidad para cada entidad

El sistema de gestión de la AC Raíz se someterá a un proceso de revisiones internas con una frecuencia anual, de los aspectos técnicos, de seguridad y operativos, de acuerdo con el Plan de Inspección elaborado por la "Dirección de Estandarización y Fiscalización en Certificación Electrónica y Seguridad de la Información" de SUSCERTE, o en el momento que se considere pertinente sin exceder mas de un año de la anterior revisión. Este proceso de revisión anual tendrá como alcance al menos, la evaluación del cumplimiento de los previsto en esta DPC y el seguimiento a observaciones realizadas en las auditorías externas anuales.

Los funcionarios de la mencionada dirección deben contar con las competencias mínimas necesarias exigidas para los auditores calificados ETSI y Webtrust, entre ellas:

- Formación y experiencia en los estándares mencionados

- Formación y experiencia en seguridad de la información
- Formación y experiencia en auditoría de tecnologías de información

Igualmente anualmente se llevará a cabo una auditoría externa para evaluar el grado de conformidad respecto a la especificación técnica ETSI TS 102 042 "Policy requirements for certification authorities issuing public key certificates" V2.4.1., teniendo en cuenta los criterios de la ETSI TS 119 403 "Trust Service Provider Conformity Assessment – Requirements for conformity assessment bodies assessing Trust Service Providers" v2.1.1.

Adicionalmente los informes deben ser consignados en lenguaje español e ingles.

16.2 Auditores

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

Cualquier persona contratada para realizar una auditoría de la AC Raíz, los PSC o los Casos Especiales, deberá cumplir con los siguientes requisitos:

- Estar inscrito en el Registro de Auditores de SUSCERTE
- Adecuada y acreditada capacitación y experiencia en ICP, seguridad y procesos de auditoría de sistemas de información.
- Independencia a nivel organizativo de la organización que gestiona la Autoridad de Certificación a ser Auditada, para el caso de auditorías externas.

Así mismo los auditores externos seleccionados para llevar a cabo las auditorías anuales deben contar con las competencias suficientes que avalan sus auditorías, a saber:

- Conocimiento de los requisitos legales, regulatorios y de cumplimiento legal en lo particular a nivel nacional y en el marco de lo establecido en CA Browser Forum (Webtrust) y ETSI 102 042.
- Conocimiento en ICP (Infraestructura de Clave Pública) y Seguridad de la Información.
- Conocimiento del Estado del Arte vigente en Infraestructura de Clave Pública.
- Conocimiento de las tecnologías aplicables a los servicios de certificación y firma electrónica, así como de Estampado de Tiempo.
- Conocimiento de la realización de las evaluaciones de riesgos de las tecnologías de información relacionada con la seguridad a fin de identificar los activos de la ICP (Infraestructura de Clave Pública), las amenazas y vulnerabilidades que proporcionan la comprensión de su ocurrencia, impacto y su mitigación.
- Conocimiento de los análisis de la vulnerabilidad de seguridad de red incluyendo pruebas de penetración.
- Conocimiento de la evaluación de los controles de seguridad de la ICP.
- Ser capaz de evaluar el funcionamiento seguro de los equipos y módulos criptográficos (norma ISO / IEC 15408).
- Haber actuado como auditor en al menos tres auditorías completas de ICP.
- Tener un conocimiento adecuado y atributos para gestionar

un proceso de auditoría.

- Competencia para comunicarse de manera efectiva, tanto de forma oral como por escrito.

16.3 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.

16.4 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 y gestión de la AC Raíz
- Gestión y distribución de las claves
- Consideraciones de Confidencialidad
- Seguridad Física y lógica
- Sistema de gestión de seguridad de la información del AC Raíz (Plan de Contingencia y Recuperación ante Desastres, Plan de Continuidad de las Actividades, entre otros)

- Personal Operativo.

16.5 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.

16.6 Comunicación del resultado

El auditor debe comunicar los resultados de la auditoría al AAP, a la máxima autoridad de la Superintendencia de Servicios de Certificación Electrónica y a los responsables de las distintas áreas en las que se detecten no conformidades.

17 REQUISITOS COMERCIALES Y LEGALES

17.1 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.

17.1.1 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).

17.1.2 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).

17.1.3 Tasas de registro por los certificados otorgados por PSC extranjeros

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

17.1.4 Tasas de acceso a los certificados

El acceso a los certificados emitidos, dada su naturaleza pública, es libre y gratuito y por tanto no hay ninguna tarifa de aplicación sobre el mismo.

17.1.5 Tasas de acceso a la información de estado o revocación

El acceso a la información de estado o revocación de los certificados es libre y gratuita y por tanto no se aplicará ninguna tarifa.

17.1.6 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.

17.1.7 Política de reintegros

No se preveen reintegros de las cantidades entregadas para el pago de este tipo de certificados.

17.2 Política de Confidencialidad

17.2.1 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 la confidencialidad establecida legalmente 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”

17.2.2 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”

17.2.3 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 revocación o suspensión de certificados.

17.2.4 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.

17.3 Protección de la información privada/secreta

17.3.1 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.

17.3.2 Información no considerada privada

La información no tiene carácter privado, por imperativo legal (“datos públicos”), pero sólo 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.

17.3.3 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.

17.3.4 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.

17.3.5 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.

17.4 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).

17.5 Obligaciones y responsabilidad civil

17.5.1 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 electrónicamente.
- 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.

17.5.2 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 se conozca que la confidencialidad 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 veinte (20) años.

17.5.3 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.

17.5.4 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.

17.5.5 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.

17.6 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.

17.7 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.

17.7.1 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.

17.7.2 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.

17.8 Plazo y finalización

17.8.1 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.

17.8.2 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.

17.9 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 electrónicamente 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.

17.10 Modificaciones

17.10.1 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).

La modificación estará justificada desde el punto de vista técnico y

legal. Además, se establece un control de modificaciones, basado en la Política de Gestión del Cambio de la AC Raíz.

En aquellos supuestos en los que se considere por la Autoridad de Aprobación de Políticas que la modificación de la DPC no reduce materialmente la confianza que una Política de Certificación o su implementación proporcionan, ni altera la aceptabilidad de los certificados que soporta la política para los propósitos para los que se han usado, se procederá al incremento del número menor de versión del documento y el último número de Identificador de Objeto (OID) que lo representa, manteniendo el número mayor de la versión del documento, así como el resto de su OID asociado. No se considera necesario comunicar este tipo de modificaciones a los suscriptores de los certificados correspondientes de la PC o DPC modificada.

En el supuesto de que la Autoridad de Aprobación de Políticas juzgue que los cambios a la especificación vigente afecten a la aceptabilidad de los certificados para propósitos específicos se procederá al incremento del número mayor de versión del documento y la puesta a cero del número menor de la misma. También se modificarán los dos (2) últimos números del de Identificador de Objeto (OID) que lo representa.

17.10.2 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 https://acraiz.suscerte.gob.ve

17.10.3 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.

17.11 Resolución de Conflictos

17.11.1 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.

17.11.2 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.

17.12 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.

17.13 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 15.13

Anexo N° 1

Huella Digital

Certificado de la AC RAÍZ SUSCERTE SHA 384	
Base 64	e54962fe5464d0b7d65dac8b8b3ffe1efc482dfb CERTIFICADO-RAIZ-SHA384
Formato Texto	e2cdd74e73feab0f72a2aa65ac88aa04a9dbf3cf CERTIFICADO-RAIZ-SHA384.txt
Formato PEM	e54962fe5464d0b7d65dac8b8b3ffe1efc482dfb CERTIFICADO-RAIZ-SHA384.crt
Formato DER	398ebe9c0f46c079c3c7afe07a2fdd9fae5f8a5c CERTIFICADO-RAIZ-SHA384.cer