GACETA OFICIAL
DE LA REPÚBLICA BOLIVARIANA DE VENEZUELA

AÑO CXLV - MES VI | Caracas, miércoles 21 de marzo de 2018 | Número 41.365

SUMARIO

Calendario Anual de reuniones Ordinarias – Año 2018

Enero	**Febrero 27**	**Marzo 20**	**Abril 24**
Mayo 29	**Junio 26**	**Julio 31**	**Agosto Vacaciones**
Septiembre 25	**Octubre 30**	**Noviembre 27**	**Diciembre 11**

Artículo 2-. El presente Acuerdo entrará en vigencia a partir del veinte (20) del mes de febrero del año 2018.

COMUNÍQUESE Y PUBLÍQUESE,

HUGBEL RAFAEL ROA CARUCI
Presidente del
Consejo Nacional de Universidades

ASALIA R. VENEGAS S.
Secretaria Permanente

CONSULTORÍA JURÍDICA MPPEUCT VISTO

REPÚBLICA BOLIVARIANA DE VENEZUELA
MINISTERIO DEL PODER POPULAR PARA
EDUCACIÓN UNIVERSITARIA, CIENCIA Y TECNOLOGÍA
SUPERINTENDENCIA DE SERVICIOS DE CERTIFICACIÓN ELECTRÓNICA

Caracas, 26 de febrero de 2018

207º, 158º y 19°

Quien suscribe, **LUIS FERNANDO PRADA FUENTES**, titular de la cédula de identidad N° **V-17.059.842**, designado como Superintendente de Servicios de Certificación Electrónica, según nombramiento contenido en la Resolución N° 095, de fecha 19 de junio de 2017, publicada en la Gaceta Oficial de la República Bolivariana de Venezuela N° 41.177, de fecha 21 de junio de 2017; en ejercicio de las atribuciones conferidas en el artículo 22, numeral 1 y 2 del Decreto con Fuerza de Ley Sobre Mensajes de Datos y Firmas Electrónicas, publicado en la Gaceta Oficial de la República Bolivariana de Venezuela N° 37.148, de fecha 28 de febrero de 2001; de conformidad con lo previsto en los artículos 4, 10, 12 y 26 del Decreto con Rango, Valor y Fuerza de Ley Orgánica de la Administración Pública, publicado en la Gaceta Oficial de la República Bolivariana de Venezuela Extraordinario N° 6.147, de fecha 17 de noviembre de 2014; y con el artículo 72 de la Ley Orgánica de Procedimientos Administrativos, publicada en la Gaceta Oficial de la República de Venezuela N° 2.818 Extraordinario, de fecha 01 de julio de 1981, en observancia con los estándares Internacionales que rigen la materia; dicta la siguiente:

PROVIDENCIA ADMINISTRATIVA Nº 001 -2018

Artículo 1. La presente Providencia Administrativa, tiene por objeto describir la Infraestructura Nacional de Certificación Electrónica, su estructura, certificados y listas de certificados revocados; conforme a los lineamientos establecidos por la Superintendencia de Servicios de Certificación Electrónica **(SUSCERTE)**. Así mismo, contempla la estructura mínima necesaria que deben tener los certificados y los valores que deben estar presentes en sus campos con el propósito de mantener la coherencia en los perfiles generados por los PSC acreditados ante la Superintendencia.

De conformidad con lo dispuesto en el artículo 22, numerales 1° y 5° y el artículo 27 del Decreto con Fuerza de Ley sobre Mensaje de Datos y Firmas Electrónicas; en concordancia con el artículo 36 del Reglamento Parcial Del Decreto Ley Sobre Mensajes de Datos y Firmas Electrónicas.

Artículo 2. La Superintendencia de Servicios de Certificación Electrónica (SUSCERTE), define en la presente providencia los aspectos técnicos de la Infraestructura Nacional de Certificación Electrónica, los certificados creados y emitidos bajo la misma; detalla su clasificación, valores, estructura y organización interna; especifica los requerimientos de las listas de certificados revocados y su estructura interna, según el procedimiento identificado como **NORMA SUSCERTE 032-06/17** edición 3.2 de fecha 30 de Junio de 2017; cuyo tenor es el siguiente:

"INFRAESTRUCTURA NACIONAL DE CERTIFICACIÓN ELECTRÓNICA: ESTRUCTURA, CERTIFICADOS Y LISTAS DE CERTIFICADOS REVOCADOS"

NORMA SUSCERTE Nº 032-06/2017, EDICIÓN Nº: 3.2, FECHA: 06/2017

1. PRELIMINARES

1.1. Objeto y Campo de Aplicación

La presente norma describe la Infraestructura Nacional de Certificación Electrónica, su estructura, certificados y listas de certificados revocados; conforme a los lineamientos presentados por la Superintendencia de Servicios de Certificación Electrónica (SUSCERTE).

Así mismo, se presenta la estructura mínima necesaria que deben tener los certificados y los valores que deben estar presentes en sus campos con el propósito de mantener la coherencia en los perfiles generados por los PSC acreditados ante la Superintendencia.

1.2. Referencias Normativas

.- Constitución de la República Bolivariana de Venezuela.

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

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

.- Providencia Administrativa Nº 016 de SUSCERTE (Febrero 2007).

.- ITU-T Rec. X.509 V.3 Tecnología de la Información. Interconexión de Sistemas abiertos - El Directorio: Marcos para certificados de claves públicas y atributos (2008).

.- RFC 5280 PKIX Certificate and CRL Profile (2008).

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

.- RFC 3739 Internet X.509 Public Key Infrastructure: Qualified Certificates Profile (2004).

.- RFC 3279 Algorithms and Identifiers for the Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile (2002).

.- 3erd Generation Partnership Project; Technical Specification Group Core Network and Terminals; Numbering, addressing and identification 3GPP TS 23.003.

1.3. Definiciones y Terminologías

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

CERTIFICADO ELECTRÓNICO	Mensaje de Datos proporcionado por un Proveedor de Servicios de Certificación (PSC) que le atribuye certeza y validez a la firma electrónica.
IDENTIFICADOR DE OBJETO	Valor universal único asociado a un objeto para identificarlo inequívocamente.
FUNCIÓN HASH	Es una función computable mediante un algoritmo, que tiene como entrada un conjunto de elementos, que suelen ser cadenas de caracteres, y los convierte (mapea) en un rango de salida finito, normalmente cadenas de longitud fija.
LISTA DE CERTIFICADOS REVOCADOS	Documento mantenido y publicado por una Autoridad de Certificación (AC) que enumera los certificados revocados por ella.
SIGNATARIO	Entidad identificada en un certificado electrónico, quien usa la clave privada para firmar electrónicamente, y que se encuentra asociada con la clave pública del certificado.
SUSCRIPTOR	Persona que contrata la generación de un certificado electrónico con un proveedor de servicios de certificación.

1.4. Símbolos y Abreviaturas

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

AC	Autoridad de Certificación.
AR	Autoridad de Registro.
ASN.1	Abstract Syntax Notation One – Notación de Sintaxis Abstracta Uno.
DPC	Declaración de Prácticas de Certificación.
GSM	Sistema global para las comunicaciones móviles, es un sistema estándar ampliamente utilizado en redes de telefonía celular de segunda, tercera y cuarta generación.
HSM	Hardware Security Module. (Módulo de Seguridad de Hardware)
IMEI	Identidad internacional de equipo móvil, es un código USSD pregrabado en los teléfonos móviles GSM. Código que identifica unívocamente al dispositivo móvil y es transmitido por éste una vez que se ha conectado a la red a la cual pertenezca.
ITU-T	International Telecommunications Union-Telecommunications. (Unión Internacional de Telecomunicaciones.)
LCR	Lista de Certificados Revocados.
LSMDFE	Ley Sobre Mensajes de Datos y Firmas Electrónicas.
OID	Identificador de Objeto.
OCSP	Online Certificate Status Protocol (Protocolo de estado de certificados en línea).
PC	Política de Certificados.
PSC	Proveedor de Servicios de Certificación.
RBV	República Bolivariana de Venezuela.
RPLSMDFE	Reglamento Parcial de Ley Sobre Mensajes de Datos y Firmas Electrónicas.
SUSCERTE	Superintendencia de Servicios de Certificación Electrónica.
URI	Uniform Resource Identifier (Identificador de recurso uniforme)
USSD	Servicio suplementario de datos no estructurados, es un servicio para el envío de datos a través de dispositivos móviles GSM.
MAC	*Media Access Control*, es un identificador de 48 bits (6 bloques hexadecimales) que corresponde de forma única a un dispositivo de red. Se conoce también como dirección física. Está determinada y configurada por el IEEE (los últimos 24 bits) y el fabricante (los primeros 24 bits) utilizando el *Organizationally Unique Identifier*.

2. DESARROLLO

2.1. Consideraciones Generales

2.1.1 La presente norma tiene como principio describir los aspectos técnicos asociados a la Infraestructura Nacional de Certificación Electrónica, los certificados creados y emitidos bajo la misma; detallar su clasificación, valores, estructura y organización interna; especificar los requerimientos de las listas de certificados revocados y su estructura interna.

2.1.2 Para la selección del modelo de la Infraestructura Nacional de Certificación Electrónica, se realizó un estudio de las diferentes topologías de Infraestructura de Claves Públicas, seleccionándose el modelo jerárquico con una Autoridad de Certificación Raíz única nacional de la cual dependen los Proveedores de Servicios de Certificación Acreditados y los Casos especiales.

2.1.3 Este modelo de arquitectura jerárquica, debe ser adoptado por todo Proveedor de Servicios de Certificación (PSC) que desee solicitar su acreditación ante SUSCERTE.

2.1.4 En la Figura Nº 1 se establecen las relaciones de confianza basadas en la arquitectura jerárquica con una única raíz de la Infraestructura Nacional de Certificación Electrónica.

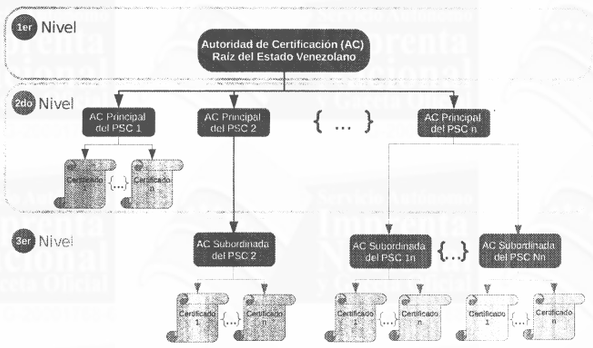

Figura Nº 1. *Modelo de Jerarquía.*

2.1.5 SUSCERTE es el ente rector y responsable de la Infraestructura Nacional de Certificación Electrónica, a través de la Autoridad de Certificación Raíz del Estado Venezolano.

2.1.6 La relación de confianza sólo se especifica en una dirección. La Autoridad de Certificación Raíz es quien emite los certificados a los PSC y estos a su vez pueden generar y emitir certificados a usuarios finales o AC subordinadas, más no pueden emitir certificados a su AC superior.

2.1.7 En la arquitectura jerárquica de la Infraestructura Nacional de Certificación Electrónica, se permite que los PSC constituyan por debajo de ellos un solo nivel de AC subordinadas.

2.1.8 Con el fin de segmentar los riesgos, un PSC que constituya al menos una AC subordinada no podrá emitir certificados a usuarios finales con su AC principal, de manera que si una de estas se ve comprometida no afectará a las otras.

2.1.9 No existe otra AC que pueda firmar el certificado de la AC Raíz. Este es el único caso en el que la AC raíz crea un certificado autofirmado.

2.1.10 La AC Raíz firma los certificados electrónicos de las AC principales de los PSC, AC de casos especiales, su Lista de Certificados Revocados (LCR) y certificado del servicio OCSP de la AC raíz.

2.1.11 La AC Raíz genera y firma los certificados de la AC principal de los PSC éstos PSC, a su vez, generan y firman los certificados de usuarios finales o de sus AC subordinadas y estas sólo generan y firman los certificados de sus usuarios finales.

2.1.12 La AC Raíz establece las condiciones para los tipos de certificados que pueden emitir las AC de los PSC.

2.2. Consideraciones Específicas

2.2.1 Cada PSC debe contar con una AC principal y una o varias AR encargadas de atender a su comunidad de usuarios.

2.2.2 Los PSC son responsables de la gestión (generación, suspensión y revocación) de los certificados electrónicos de sus signatarios y no de los usos posteriores que estos le den a los certificados. Sin embargo, los PSC deben velar por el buen uso de los certificados en función de las obligaciones que el signatario asume como usuario del servicio de certificación de acuerdo al Decreto con Fuerza Ley Sobre Mensaje de Datos y Firmas Electrónicas.

2.2.3 Los PSC pueden gestionar varios tipos de certificados de acuerdo al tipo de signatario:

a) Certificados de AC: son los únicos que se pueden utilizar para firmar otras AC o certificados de usuario final, se deben tener condiciones especiales de generación y resguardo de los mismos.

b) Certificado para Personas: cuando el signatario sea una persona, quien en nombre propio o representación de tercero, y previa validación de la identidad y del suscriptor ante la autoridad que expide el certificado, solicita la generación del mismo, con lo cual tendrá a su disposición el certificado electrónico mediante el uso de dispositivos criptográficos para tal fin (tarjeta inteligente, token USB, entre otros) o de software.

c) Certificado para Sistemas: serán usados por componentes, equipos y/o dispositivos que requieran o no de la intervención directa de la persona. El certificado reside en un almacén basado en software o hardware.

d) Certificados para Operaciones de ICP: destinados a las operaciones y servicios requeridas para el funcionamiento óptimo de la AC y/o AR del AC raíz, AC Principales y AC Subordinadas.

Todos los certificados deben ser evaluados y aprobados por parte de SUSCERTE utilizando esta norma como directriz.

2.2.4 Los tipos de certificados electrónicos a ser emitidos por los PSC deben cumplir con lo establecido en la presente Norma y en los estándares en la materia, someterse a la consideración, evaluación y aprobación por parte de SUSCERTE, a efectos de asegurar su interoperabilidad en la Infraestructura Nacional de Certificación Electrónica.

2.2.5 Los tipos de certificados, los dispositivos para la generación y almacenamiento del par de claves, la vigencia y el tamaño mínimo del par de claves se muestran en la Tabla Nº 1.

Tabla Nº 1. *Tipos de Certificados, dispositivo, almacenamiento, vigencia y tamaño del par de claves*

PARA AUTORIDADES DE CERTIFICACIÓN			
Tipo de Certificado	**Dispositivo para Generación y Almacenamiento del par de claves**	**Vigencia Máxima en años**	**Tamaño Mínimo del par de claves (bits)**
AC Raíz	Hardware (HSM)	20	4096
AC Principal PSC		10	4096
AC Subordinada PSC		5	4096
AC Caso Especial		1	4096

PARA USUARIO FINAL			
Tipo de Certificado	**Dispositivo para Generación y Almacenamiento del par de claves**	**Vigencia Máxima en meses**	**Tamaño Mínimo del par de claves (bits)**
Para persona	Software	12	2048
	Hardware (token criptográfico, tarjeta inteligente)	24	2048
Para software o aplicaciones	Software	12	2048
	Hardware (HSM)	24	2048

2.2.6 Es obligatorio el uso de HSM para la generación y el almacenamiento del par de claves para los certificados de la AC Raíz, AC Principal del PSC, AC Subordinadas del PSC y AC Caso Especial.

2.2.7 Los procedimientos para las solicitudes y emisiones de los pares de claves, se especificarán en la Declaración de Prácticas de Certificación (DPC) del PSC y en las PC.

2.2.8 Los procedimientos en caso de pérdida, reemplazo o renovación de algún certificado, se establecerán en la DPC y/o PC del PSC.

2.2.9 El signatario y suscriptor deben conocer las políticas de uso de los certificados electrónicos establecidas por el PSC para dar curso a las buenas prácticas y al uso permitido de los mismos. Para ello, el PSC deberá promover que los signatarios y suscriptores conozcan dichas políticas. En caso de menores de edad se someterá a la evaluación del carácter legal del certificado por parte de SUSCERTE y el PSC, para los casos que se presenten. En el caso de extranjeros serán identificados en el certificado electrónico con su número de pasaporte.

2.3. Procedimiento General

2.3.1 Los certificados generados y firmados bajo la Infraestructura Nacional de Certificación Electrónica son los definidos para X.509v3, así como lo establecido en el RFC 3739 (Internet X.509 Public Key Infrastructure, Qualified Certificates Profile). Dicho estándar define la siguiente estructura general: Datos del certificado, Datos del emisor, Periodo de validez, Datos del titular, Información de clave pública y Extensiones.

2.3.2 En la sección de Datos del Certificado se debe incluir la versión, serial y algoritmo de firma.

2.3.2.1 La versión contemplada para los certificados emitidos en la Infraestructura Nacional de Certificación Electrónica es la Versión 3 (Indicado por el entero 2).

2.3.2.2 El serial, contemplado en los Datos del Certificado, es el valor entero único asignado por la AC al emitir el certificado. Puede ser expresado en formato hexadecimal de 20 octetos. Este valor no puede ser negativo.

2.3.2.3 El algoritmo de firma es el algoritmo SHA256 para los Certificados Electrónicos de Entidad Final con longitud de cifrado de 2048bits y para los Certificados Electrónicos de AC la longitud de cifrado es de 4096bits.

2.3.3 El Emisor (issuer) del certificado contiene información que identifica unívocamente al PSC emisor del certificado electrónico. Dicha información es de tipo *Distinguished Name.*

2.3.3.1 La nomenclatura que debe utilizarse para los campos de tipo nombre distinguido (Distinguished Name - DN). Los atributos utilizados para identificar al emisor y titular del certificado son definidos por el RFC 3739 (Ver Anexo C).

2.3.3.2 El DN Serial Number (serialNumber) debe identificar al PSC a través del R.I.F. (Ver Anexo A).

2.3.4 La validez del certificado contiene la fecha exacta de emisión (noBefore) y de expiración del certificado (noAfter). Debe ser expresada en formato UTC (GMT 0) y coincidir con los límites establecidos por esta norma (Ver Vigencia en la Tabla N° 1).

2.3.5 El Titular (subject) del certificado contiene información que identifica unívocamente al mismo del certificado electrónico. Dicha información es de tipo Distinguished Name. El formato de dicho campo al igual que en Distinguished Name y se debe garantizar que dichos atributos lo distingan unívocamente.

2.3.6 La Información de Clave Pública del Titular deberá especificar el algoritmo y otras características del cifrado de la misma.

2.3.7 Las extensiones de los certificados constituyen métodos para asociar información del certificado, emisor y titular. Dichas extensiones pueden ser carácter crítico o no crítico, que le permite ser ignorada o no por un sistema.

2.3.7.1 Como mínimo, los certificados, deben poseer las siguientes extensiones: Restricciones Básicas, Clave de Uso, Identificador de clave de Titular, Identificador de clave de Autoridad Certificadora, Clave de Usos Extendidos, Nombre Alternativo del Titular, Nombre Alternativo del Emisor, Puntos de Distribución de las LCR, Acceso a la Información de Autoridad (AIA) y Política de Certificación (PC).

2.3.7.2 La extensión Restricciones Básicas (basicConstrain) es de carácter crítico, determina si el certificado será utilizado como AC y especifica si puede firmar otra AC.

2.3.7.3 La extensión Clave de Uso (Key Usage) es de carácter crítico y puede tener los siguientes valores habilitados: Firma digital, Compromiso con el Contenido, Cifrado de claves, Cifrado de datos, Acuerdo de claves, Firma de certificado, Firma de LCR, Solo cifrado y Solo descifrado (Ver Anexo D).

Las Claves de Uso: Firma de Certificado y Firma de LCR están reservadas exclusivamente a los certificados de AC raíz, AC principal y AC subordinada.

La Clave de Uso "No Repudio" fue renombrada "Compromiso o Vinculación con el Contenido". Para la elaboración de Políticas de Certificación se debe utilizar "Compromiso con el Contenido".

2.3.7.4 El Identificador de Clave de Titular contiene el resultado de la Función Hash sobre la Clave Pública del Titular.

2.3.7.5 El Identificador de clave de Autoridad Certificadora contiene el resultado de la Función Hash sobre la Clave Pública de la Autoridad de Certificación, Nombre y Serial de la misma.

2.3.7.6 La Clave de Uso Extendido puede ser de carácter crítico o no crítico y complementan la funcionalidad de un certificado. El PSC podrá incorporar tantos Usos de Clave Extendidos como sean necesarios de acuerdo a la Política de Certificación. Ver Anexo E.

2.3.7.7 Nombre Alternativo del Titular, es una extensión de carácter no crítico. Debe contener uno o más nombres alternativos en formato de Nombres Generales (General Name – GN). Ver la Anexo B.

2.3.7.8 Nombre Alternativo del Emisor, es una extensión de carácter no crítico. Debe contener uno o más nombres alternativos en formato de Nombres Generales (General Name – GN). Ver la Anexo B.

2.3.7.9 En Puntos de Distribución de las LCR se deben colocar al menos un punto para poder validar el estatus del certificado.

2.3.7.10 El Acceso a la Información de la Autoridad (Authority Info Access) está destinada a contener el método y URL donde se puede consultar el estatus del certificado. Estos pueden ser servicios como LDAP, OCSP y otras soportadas por el estándar X.509.

2.3.7.11 Las Políticas de Certificación deben contener información que identifique las políticas bajo las cuales fue emitido el certificado y donde se puede obtener dicha documentación.

Si el PSC contiene más de una política u otra documentación en la ubicación a la que hace referencia en esta extensión, debe proveer información que permita reconocer exactamente a cuál PC está asociada el certificado.

2.3.7.1 Las limitaciones de uso de cada tipo de certificado deben estar establecidas en su correspondiente política de certificados.

2.3.8 La Lista de Certificados Revocados es un instrumento de validación del estatus de un certificado electrónico definido en el RFC 5280. Esta contiene los números seriales, fecha y motivo de suspensión y/o revocación de los certificados electrónicos. Estos deben estar ordenados por tiempo de ingreso a la lista y deben permanecer en ella a pesar de expirar por motivos de seguridad.

2.3.9 Todo campo que no este clasificado en la estructura del certificado (Anexo J) como opcional, es obligatorio.

2.3.10 En caso de que el PSC o Caso Especial estimen, en sus políticas de certificados campos adicionales a los obligatorios por esta Norma, para la estructura de los certificados electrónicos y de la LCR, deben ceñirse a lo estipulado como campos opcionales tanto en su denominación como uso.

2.3.11 En caso de que el PSC o Caso Especial estimen, en sus políticas de certificados campos adicionales a los obligatorios por esta Norma, para la estructura de los certificados electrónicos y de la LCR, y ninguno de los campos opcionales estipulados cumplan en su denominación y uso, quedará a juicio de SUSCERTE aprobar su empleo o no en función de los estándares internacionales.

3. PARTE FINAL

3.1. Disposiciones transitorias

PRIMERA: A partir de la fecha de publicación en gaceta de esta Norma, se deberá iniciar un proceso de actualización de sus políticas de certificación y las plantillas de los certificados electrónicos que no cumplan con lo aquí previsto, por parte de los Proveedores de Servicio de Certificación (PSC) acreditados, a tales efectos se estima un período de 12 meses contados a partir de su publicación. Durante ese lapso el PSC debe consignar ante SUSCERTE informes trimestrales donde se evidencie el alcance y avance de esta actualización. De igual forma, SUSCERTE como parte de este proceso de actualización por parte de los PSC, debe realizar la asignación de los OID requeridos para permitir dichas actualizaciones.

SEGUNDA: Para que los certificados de la Cadena de Confianza Nacional cumplan con lo establecido en esta Norma, los certificados electrónicos de las autoridades de certificación (AC Raíz, AC Principal de los PSC, AC Subordinada del PSC y AC de los Casos Especiales), que estén en producción, pasaran por un proceso de migración iniciándo por la AC Raíz, a través del cual se generarán nuevos certificados electrónicos a las autoridades de certificación.

3.2. Disposiciones finales

Si los estándares y recomendaciones internacionales utilizados para la elaboración de esta norma son actualizados o reemplazados, SUSCERTE puede solicitar a los PSC aplicar dichos cambios a fin de garantizar el funcionamiento óptimo de la Infraestructura Nacional de Certificación Electrónica.

Para los casos en que no se hace una mención explícita sobre un aspecto en particular, se debe utilizar como recomendación, lo establecido en las referencias normativas de este documento.

4. ANEXOS

Los anexos constituyen parte integral de la norma y deben ser de cumplimiento obligatorio por los PSC.

4.1 Anexo A: Uso del *DN Serial Number*

Se debe utilizar para identificar unívocamente al emisor, titular y/o propietario del certificado electrónico. Es responsabilidad de la Autoridad de Registro verificar que se aplique el correspondiente según esta norma y la PC bajo la cual se emitió el certificado.

Para identificar personas se debe utilizar la Cédula de Identidad (C.I.), Registro Único de Información Fiscal (R.I.F) o Número de Pasaporte.

Para identificar organizaciones y empresas públicas o privadas se debe utilizar el Registro Único de Información Fiscal (R.I.F).

Para identificar dispositivos, sistemas o componentes de sistema se deben utilizar la Dirección MAC, DNS, IMEI según sea el caso.

Como última opción SUSCERTE podrá asignar y autorizar la utilización de Identificador de Objeto Único (OID) para distinguir al sujeto.

La cédula de identidad deberá incluir en un literal la nacionalidad del titular (V o E) y los dígitos que lo identifican en el siguiente formato: V-00000000 o E-00000000 según sea el caso.

El Registro Único de Información Fiscal deberá seguir el formato del ente emisor, ejemplo: V-00000000, G-000000000, J-000000000

El Pasaporte deberá incluir todos los dígitos de dicho documento.

DNS o Sistema de Dominio de Nombres identifica de manera jerárquica a sistemas conectados a internet.

La dirección MAC es definida por 48 bits que identifican de manera única al dispositivo de red. Se compone de 6 bloques en formato hexadecimal de la siguiente manera xx-xx-xx-xx-xx-xx o xx:xx:xx:xx:xx:xx.

El código IMEI debe tener de 15 a 16 dígitos basado en el estándar internacional 3GPP TS 23.003.

4.2 Anexo B: Nombres Generales

Nombre	X.509	Tipo de Dato
Otro Nombre	otherName	OtherName
Nombre RFC822	rfc822Name	IA5String
Nombre DNS	dNSName	IA5String
Dirección X400	x400Address	ORAddress
Nombre de Directorio	directoryName	Name
Nombre de Identificación de Datos Electrónicos	ediPartyName	EDIPartyName
Identificador Uniforme de Recursos	uniformResourceIdentifier	IA5String
Dirección IP	iPAddress	OCTET STRING
ID registrada	registeredID	OBJECT IDENTIFIER

4.3 Anexo C: Nombres Distinguidos

Nombre	X.509	O.I.D.
Nombre Común	commonName	2.5.4.3
Organización	organization	2.5.4.10
Departamento	organizationalUnity	2.5.4.11
País	country	2.5.4.6
Correo Electrónico	emailAddress	1.2.840.113549.1.9.1
Localidad	locality	2.5.4.7
Estado	state	2.5.4.8
Título	title	2.5.4.12
Teléfono	telephoneNumber	2.5.4.20
Categoría de Negocio	businessCategory	2.5.4.15
Nombre	givenName	2.5.4.42
Apellido	surName	2.5.4.4
Identificador de documento	documentIdentifier	0.9.2342.19200300.100.1.11
Serial	serialNumber	2.5.4.5
Iniciales	initials	2.5.4.43
Descripción	description	2.5.4.13
Propietario	owner	2.5.4.32
Título de Documento	documentTitle	0.9.2342.19200300.100.1.12
Hospedaje	host	0.9.2342.19200300.100.1.9
Calle(Dirección)	streetAddress	2.5.4.9
Código Postal	postalCode	2.5.4.17
Dirección Postal	postalAddress	2.5.4.16

4.4 Anexo D: Claves de Uso

Nombre de Uso	X.509 (bit)	Observación
Firma Digital	digitalSignature(0)	Permite realizar la operación de firma electrónica
Compromiso con el Contenido (Anteriormente No Repudio)	contentCommitment(1)	nonRepudiation(1) – fue renombrado este bit a contentCommitment [RFC3280]. Función que se usa para dar a conocer que el firmante ha comprendido lo que firma y manifiesta la intención de firmar el compromiso del contenido.
Cifrado de claves	keyEncipherment(2)	Su función consiste en la gestión y transporte de claves para establecer sesiones seguras
Cifrado de datos	dataEncipherment(3)	Se usa para cifrar datos del usuario que no sean claves criptográficas
Acuerdo de claves	keyAgreement(4)	Cifra el mensaje entre el transmisor y el receptor, usada con cifrado Diffie-Hellman.
Firma de certificado	keyCertSign(5)	Permite a las ACs, firmar certificados electrónicos. Utilizada cuando la clave pública es usada para verificar una firma en un certificado.
Firma de LCR	cRLSign(6)	Se activa el bit cRLSign cuando la clave pública se usa para verificar una firma en la lista de certificados revocados. (Ejemplo: CRL, delta CRL o ARL).
Solo cifrado	encipherOnly(7)	Habilita la clave pública solo para cifrar datos mientras se ejecuta el acuerdo de claves.
Solo descifrado	decipherOnly(8)	Habilita la clave pública solo para descifrar datos mientras se ejecuta el acuerdo de claves.

4.5 Anexo E: Claves de Usos Extendidos

A continuación se presentan diferentes Claves de Usos Extendidos que pueden añadir funcionalidades a los certificados electrónicos.

Nombre	X.509 (bit)	OID
Autenticación de Servidor	serverAuth	1.3.6.1.5.5.7.3.1
Autenticación de Cliente	clientAuth	1.3.6.1.5.5.7.3.2
Firma de Código	codeSigning	1.3.6.1.5.5.7.3.3
Protección Correo Electrónico	emailProtection	1.3.6.1.5.5.7.3.4
Estampado de Tiempo	timeStamping	1.3.6.1.5.5.7.3.8
Firma de OCSP	ocspSigning	1.3.6.1.5.5.7.3.9
EAP over PPP	eapOverPPP	1.3.6.1.5.5.7.3.13
EAP over LAM	eapOverLAN	1.3.6.1.5.5.7.3.14
Server based certification validation protocol responder	scvpServer	1.3.6.1.5.5.7.3.15
Server based certification validation protocol responder	scvpClient	1.3.6.1.5.5.7.3.16
Internet Key Exchange	ipSecike	1.3.6.1.5.5.7.3.17
Secure Shell Authentication Client	sshClient	1.3.6.1.5.5.7.3.21
Secure Shell Authentication Server	sshServer	1.3.6.1.5.5.7.3.22
Microsoft Smart Card Logon	smartCardLogon	1.3.6.1.4.1.311.20.2.2
Microsoft Document Signing	documentSigning	1.3.6.1.4.1.311.10.3.12
Microsoft Individual Code Signing	individualCodeSigning	1.3.6.1.4.1.311.2.1.21
Microsoft Comercial Code Signing	comercialCodeSingning	1.3.6.1.4.1.311.2.1.22
Microsoft Encrypted File System	encryptedFileSystem	1.3.6.1.4.1.311.10.3.4
Microsoft Encrypted File System Recovery	encryptedFileSystemRecovery	1.3.6.1.4.1.311.10.3.4.1
Adobe PDF Signing	adobePdfSigning	1.2.840.113583.1.1.5

4.6 Anexo F: Perfil de Lista de Certificados Revocados (LCR)

Perfil de Lista de Certificados Revocados		
Nombre(X.509)	**Tipo de dato [Constante] < Valor >**	**Crítica (para extensiones)**
Datos de LCR		
Versión (version)	Entero Hexadecimal [V2] < 0x1 >(Representa la versión 2 del X.509)	
Algoritmo de Firma (signature)	Algoritmo Autorizado	
Datos de Emisor (issuer)		
Nombre Común (commonName)	<Identificación de la AC Principal del Proveedor de Servicios de Certificación>	
Correo Electrónico (emailAddress)	<Correo electrónico de la AC >	
Teléfono (telephoneNumber)	<Número de teléfono local del emisor>(Opcional)	
Departamento (organizationalUnity)	<Nombre o razón social tal cual aparezca en el documento constitutivo del emisor>	
Organización (organization)	[Sistema Nacional de Certificación Electrónica]	
Localidad (locality)	<Dirección física del emisor>	
Estado	<Estado en el cual se ubica el emisor >	
País	[VE]	

Datos de Validez		
Última Fecha de Actualización (thisUpdate o lastUpdate)	Fecha (UTC)	
Siguiente Fecha de Actualización (nextUpdate)	Fecha (UTC)	
Extensiones de LCR		
Identificador de clave de Autoridad Certificadora (Authority Key Identifier)		
Clave de Autoridad (keyIdentifier)	KeyIdentifier <Identificador de la clave pública de la AC Raíz>	
Nombre distintivo (authorityCertIssuer)	GeneralName <Contiene la información de la AC Raíz con el formato DN >	
Serial (authorityCertSerialNumber)	CertificateSerialNumber <Contiene el número del certificado del emisor>	
Certificados Revocados		
Certificados revocados (Revoked Certificates)		
Serial del Certificado (Serial Number)	Entero Hexadecimal <Serial de certificado a revocar >	
Fecha de revocación (Revocation Date)	Fecha <fecha y hora en formato UTC>	
Razón de Revocación (CRL Reason Code)	Razón de Revocación < Ver Anexo G >	
Firma		
Algoritmo de Firma (signatureAlgorithm)	Algoritmo Autorizado	
Firma(signature)	<Contenido de la Firma>	

4.7 Anexo G: Razón de Revocación

Se utilizan para indicar la razón de revocación de un certificado en la LCR.

Nombre	X.509
Sin Especificar	unspecified
Compromiso de Clave	keyCompromise
Compromiso de AC	cACompromise
Cambio de Afiliación	affiliationChanged
Sustitución	superseded
Cese de operaciones	cessationOfOperation
Retención de Certificado	certificateHold
Borrado de LCR	removeFromCRL
Retiro de privilegios	privilegeWithdrawn
Compromiso de AA	aACompromise

4.8 Anexo H: Directorio de Nombres del Titular (Subject Directory Name)

Es una extensión del certificado que contiene atributos que describen al titular del mismo.

Nombre	X.509	Observación
Fecha de Nacimiento	dateOfBirth	Indica la fecha de nacimiento del Titular
Lugar de Nacimiento	placeOfBirth	Indica el lugar de nacimiento del Titular
Género	gender	El tamaño del campo es de 1, puede contener solo "M", "m", "F" o "f".
País de Ciudadanía	countryOfCitizenship	El tamaño del campo es de 2 y debe contener el código de país en ISO 3166. Ejemplo "VE"
País de Residencia	countryOfResidence	El tamaño del campo es de 2 y debe contener el código de país en ISO 3166. Ejemplo "VE"

4.9 Anexo I: Información de Datos Biométricos (Biometric Data Info)

Es una extensión del certificado que contiene información que permite relacionar al titular con sus datos biométricos.

Nombre	X.509	Observación
Tipo de datos biométrico	typeOfBiometricData	Describe el tipo de información biométrica que hace referencia esta extensión. Por defecto es una imagen de la firma autógrafa del titular (handwritten-signature).
Algoritmo de Hash	hashAlgorithm	Es la función hash utilizada para la digerir información.
Hash de datos Biométricos	biometricDataHash	Es el resultado de la función hash de la información biométrica.
URI de la Fuente	sourceDataUri	Contiene la ubicación de dónde se almacena la información biométrica a la cual se hace referencia en esta extensión. Esta URI no implica que sea la única ubicación de dicha información.

4.10 Anexo J: Estructuras de Certificados

4.10.1 Estructura Certificado AC Raíz o Certificado Electrónico Autofirmado

Es el único certificado de la Infraestructura Nacional de Certificación Electrónica que es autofirmado y se utiliza para firmar certificados necesarios para su operación y los certificados de AC Principal de los PSC Acreditados.

Certificado de la AC Raíz		
Nombre(X.509)	**Tipo de dato [Constante] < Valor >**	**Crítica (para extensiones)**
Datos del Certificado		
Versión (version)	Entero Hexadecimal [V3] < 0x2 >(Representa la versión 3 del X.509)	
Serial (serialNumber)	Entero Hexadecimal <Asignado por la AC> (No negativo)	
Algoritmo de Firma (signature)	Algoritmo Autorizado (OID de los algoritmos permitidos como mínimo SHA384withRSAEncryption o SHA512withRSAEncryption o Superior)	
Datos de Emisor (issuer)		
Nombre Común (commonName)	UTF8 [Autoridad de Certificación Raíz del Estado Venezolano]	
Correo Electrónico (emailAddress)	UTF8 [acraiz@suscerte.gob.ve]	
Teléfono (telephoneNumber)	UTF8 <Teléfono de contacto> (Opcional)	
Departamento (organizationUnity)	UTF8 [Superintendencia de Servicios de Certificación Electrónica]	
Organización (organization)	UTF8 [Sistema Nacional de Certificación Electrónica]	
Localidad (locality)	UTF8 <Dirección física de SUSCERTE>	
Estado (state)	UTF8 <Estado en el cual se ubica SUSCERTE>	
País (country)	UTF8 [VE] (ISO 3166-1-alpha-2)	
Datos de Validez		
No Antes(notBefore)	Fecha (UTC)	
No Después(noAfter)	Fecha (UTC)	
Datos de Titular (subject)		
Nombre Común (commonName)	UTF8 [Autoridad de Certificación Raíz del Estado Venezolano]	
Correo Electrónico(emailAddress)	UTF8 [acraiz@suscerte.gob.ve]	
Teléfono (telephoneNumber)	UTF8 <Teléfono de contacto>(Opcional)	
Departamento (organizationUnity)	UTF8 [Superintendencia de Servicios de Certificación Electrónica]	
Organización (organization)	UTF8 [Sistema Nacional de Certificación Electrónica]	
Localidad(locality)	UTF8 <Dirección física de SUSCERTE>	
Estado(state)	UTF8 <Estado en el cual se ubica SUSCERTE>	
País(country)	UTF8 [VE] (ISO 3166-1-alpha-2)	
Información de Clave Pública del Titular (subjectPublicKey)		
Algoritmo de clave pública (algorithm)	<Algoritmo Asignado> (rsaEncryption, dhpublicnumber, id-dsa, id-ecPublicKey)	
Módulo(modulus) *	Cadena de Octetos [4096 bit]	
Exponente(exponent) *	Entero Hexadecimal [65537] <0x10001>	
* Para el caso de RSA se exigen estos campos		
Extensiones		
Restricciones Básicas (basicConstraints)		X
Autoridad de Certificación(aC)	Booleano [true]	
Claves de Usos(keyUsage)		X
Firma de certificado	keyCertSign(5)	
Firma de LCR	cRLSign (6)	
Identificador de clave de Titular (Subject Key Identifier)	**Valor hexadecimal <Hash> (Resultado de Función Hash)**	
Nombre Alternativo del Emisor (issuerAltName)		
Otro Nombre (otherName)	[RIF G-20004036-0]	
Identificador de clave de Autoridad Certificadora (Authority Key Identifier)		
Clave de Autoridad(keyIdentifier)	KeyIdentifier <Identificador de la clave pública de la AC Raíz>	
Nombre distintivo (authorityCertIssuer)	GeneralNames <Contiene la información de la AC Raíz con el formato DN>	
Serial (authorityCertSerialNumber)	CertificateSerialNumber <Contiene el número del certificado del emisor>	
Nombre Alternativo del Titular (subjectAltName)		
Nombre DNS (dNSName)	[suscerte.gob.ve]	
Puntos de Distribución de las LCR (cRLDistributionPoints)		
Punto de distribución LCR (distributionPoint)	<Dirección de descarga de la LCR por el AC RAIZ> [URI:http://www.suscerte.gob.ve/lcr]	
Punto de distribución LCR (distributionPoint)	[URI:http://acraiz.suscerte.gob.ve/lcr/]	
Punto de distribución LCR (distributionPoint)	[ldap://acraiz.suscerte.gob.ve]	
AIA (authorityInfoAccess)		
Método de Acceso (accessMethod)	1.3.6.1.5.5.7.48.1 [OCSP]	
Dirección de Acceso (accessLocation)	<Dirección del servicio del OCSP del AC RAIZ> [URI:http://acraiz.suscerte.gob.ve/ocsp/]	
AIA (authorityInfoAccess)		
Método de Acceso (accessMethod)	1.3.6.1.5.5.7.48.2 [CAI]	
Dirección de Acceso (accessLocation)	<Dirección del CERTIFICADO DE LA AUTORIDAD *.CRT>	
Políticas de Certificación (PolicyInformation) (Opcional: No aplica de acuerdo a las guías Webtrust)		
PolicyInformation (PC)		
policyIdentifier	<OID Autorizado por SUSCERTE>	
cPSuri	<Dirección dónde se puede descargar la PC>	
userNotice	(No se usa)	
PolicyInformation (DPC)		
policyIdentifier	<OID Autorizado por SUSCERTE>	
cPSuri	<Dirección dónde se puede descargar la DPC>	
userNotice	(No se usa)	
Firma		
Algoritmo de Firma (signatureAlgorithm)	Algoritmo Autorizado (OID de los algoritmos permitidos mínimo SHA384withRSAEncryption o SHA512withRSAEncryption o Superior)	
Firma(signature)	<Contenido de la Firma>	

4.10.2 Estructura Certificado AC Principal

Certificados emitidos y firmados por el AC Raíz, se utilizan para firmar certificados de AC Subordinadas o Certificados de Entidad o Usuario Final. También puede generar y firmar certificados y listas de certificados necesarias para su operación.

Certificado de AC Principal		
Nombre(X.509)	**Tipo de dato [Constante] < Valor >**	**Crítica (para extensiones)**
Datos de Certificado		
Versión (version)	Entero Hexadecimal [V3] < 0x2 >(Representa la versión 3 del X.509)	
Serial (serialNumber)	Entero Hexadecimal <Asignado por la AC> (No negativo)	
Algoritmo de Firma (signature)	Algoritmo Autorizado (OID de los algoritmos permitidos como mínimo SHA384withRSAEncryption o SHA512withRSAEncryption o Superior)	
Datos del Emisor (issuer)		
Nombre Común (commonName)	UTF8 [Autoridad de Certificación Raíz del Estado Venezolano]	
Correo Electrónico(emailAddress)	UTF8 [acraiz@suscerte.gob.ve]	
Teléfono (telephoneNumber)	UTF8 <Teléfono de contacto> (Opcional)	
Departamento (organizationUnity)	UTF8 [Superintendencia de Servicios de Certificación Electrónica]	
Organización (organization)	UTF8 [Sistema Nacional de Certificación Electrónica]	
Localidad(locality)	UTF8 <Dirección física de SUSCERTE>	
Estado(state)	UTF8 <Estado en el cual se ubica SUSCERTE>	
País(country)	UTF8 [VE] (ISO 3166-1-alpha-2)	

Datos de Validez		
No Antes(notBefore)	Fecha (UTC)	
No Después(noAfter)	Fecha (UTC)	
Datos de Titular (subject)		
Nombre Común (commonName)	UTF8 <Identificación de la AC Subordinada del Proveedor de Servicios de Certificación>	
Correo Electrónico(emailAddress)	UTF8 <Correo electrónico del ente que gestiona la AC Subordinada>	
Teléfono (telephoneNumber)	UTF8 <Teléfono de contacto del Titular>(Opcional)	
Departamento (organizationUnity)	UTF8 <Nombre o razón social tal cual aparezca en el documento constitutivo del ente que gestiona la AC Subordinada>	
Organización (organization)	UTF8 [Sistema Nacional de Certificación Electrónica]	
Localidad(locality)	UTF8 <Dirección física del PSC>	
Estado(state)	UTF8 <Estado en el cual se ubica el PSC>	
País(country)	UTF8 [VE] (ISO 3166-1-alpha-2)	
Información de Clave Pública del Titular		
Algoritmo de clave pública (algorithm)	<Algoritmo Asignado> (rsaEncryption, dhpublicnumber, id-dsa, id-ecPublicKey)	
Clave Pública de Titular (subjectPublicKey)		
Módulo(modulus) *	Cadena de Octetos [4096 bit]	
Exponente(exponent) *	Entero Hexadecimal [65537] <0x10001>	
* Para caso de RSA se exigen estos campos		
Extensiones		
Restricciones Básicas (basicConstraints)		X
Autoridad de Certificación(aC)	Booleano [true]	
Longitud de Certificación(pathLen)	Entero Hexadecimal [1] (Delimita a un nivel AC que pueden estar por debajo de ella)	
Claves de Usos(keyUsage)		X
Firma de certificado	keyCertSign(5)	
Firma de LCR	cRLSign (6)	
Identificador de clave de Titular (Subject Key Identifier)	Valor hexadecimal <Hash> (Resultado de Función Hash)	
Nombre Alternativo del Emisor (issuerAltName)		
Otro Nombre (otherName)	[RIF G-20004036-0]	
Identificador de clave de Autoridad Certificadora (Authority Key Identifier)		
Clave de Autoridad(keyIdentifier)	KeyIdentifier <Identificador de la clave pública de la AC Raíz>	
Nombre distintivo (authorityCertIssuer)	GeneralNames <Contiene la información de la AC Raíz con el formato DN>	
Serial (authorityCertSerialNumber)	CertificateSerialNumber <Contiene el número del certificado del emisor>	
Nombre Alternativo del Titular (subjectAltName)		
Nombre DNS (dNSName)	<DNS del PSC registrado en nic.ve>	
Otro Nombre (otherName)	<Código de identificación del PSC acreditado asignado por SUSCERTE>	
Otro Nombre (otherName)	<RIF del PSC>	
AIA (authorityInfoAccess)		
Método de Acceso (accessMethod)	1.3.6.1.5.5.7.48.1 [OCSP]	
Dirección de Acceso (accessLocation)	<Dirección del servicio OCSP del AC RAIZ> [URI:http://acraiz.suscerte.gob.ve/ocsp/]	
Puntos de Distribución de las LCR (cRLDistributionPoints)		
Punto de distribución LCR (distributionPoint)	<Dirección de descarga de la LCR por el AC RAIZ> [URI:http://www.suscerte.gob.ve/lcr]	
Punto de distribución LCR (distributionPoint)	[URI:http://acraiz.suscerte.gob.ve/lcr/]	
Punto de distribución LCR (distributionPoint)	[ldap://acraiz.suscerte.gob.ve]	
Políticas de Certificación (PolicyInformation)		
PolicyInformation (PC)		
policyIdentifier	<OID Autorizado por SUSCERTE>	
cPSuri	<Dirección dónde se puede descargar la PC>	
userNotice	(No se usa)	
PolicyInformation (DPC)		
policyIdentifier	<OID Autorizado por SUSCERTE>	
cPSuri	<Dirección dónde se puede descargar la DPC>	
userNotice	(No se usa)	
Firma		
Algoritmo de Firma (signatureAlgorithm)	Algoritmo Autorizado (OID de los algoritmos permitidos mínimo SHA256withRSAEncryption o SHA384withRSAEncryption o Superior)	
Firma(signature)	<Contenido de la Firma>	

4.10.3 Estructura Certificado AC Subordinada del PSC

Certificados emitidos y firmados por el AC Principal, se utilizan para firmar Certificados de Entidad o Usuario Final. También puede generar y firmar certificados y listas de certificados necesarias para su operación.

Certificado de AC Subordinada		
Nombre(X.509)	**Tipo de dato [Constante] < Valor >**	**Crítica (para extensiones)**
Datos de Certificado		
Versión (version)	Entero Hexadecimal [V3] < 0x2 >(Representa la versión 3 del X.509)	
Serial (serialNumber)	Entero Hexadecimal<Asignado por la AC> (No negativo)	
Algoritmo de Firma (signature)	Algoritmo Autorizado (OID de los algoritmos permitidos como mínimo SHA384withRSAEncryption o SHA512withRSAEncryption o Superior)	
Datos del Emisor (issuer)		
Nombre Común (commonName)	UTF8 <Identificación de la AC>	
Correo Electrónico(emailAddress)	UTF8 <Dirección de correo electrónico de contacto del Emisor>	
Teléfono (telephoneNumber)	UTF8 <Teléfono de contacto del Emisor>(Opcional)	
Departamento (organizationUnity)	UTF8 <Nombre o Razón social como aparece en documento constitutivo del PSC>	
Organización (organization)	UTF8 [Sistema Nacional de Certificación Electrónica]	
Localidad(locality)	UTF8 <Ciudad de ubicación del Emisor>	
Estado(state)	UTF8 <Estado de ubicación del Emisor>	
País(country)	UTF8 [VE] (ISO 3166-1-alpha-2)	

Datos de Validez		
No Antes(notBefore)	Fecha (UTC)	
No Después(noAfter)	Fecha (UTC)	
Datos de Titular (subject)		
Nombre Común (commonName)	UTF8 <Identificación de la AC Principal del Proveedor de Servicios de Certificación>	
Correo Electrónico(emailAddress)	UTF8 <Correo electrónico de la AC del PSC >	
Teléfono (telephoneNumber)	UTF8 <Teléfono de contacto>(Opcional)	
Departamento (organizationUnity)	UTF8 <Nombre o razón social tal cual aparezca en el documento constitutivo del PSC >	
Organización (organization)	UTF8 [Sistema Nacional de Certificación Electrónica]	
Localidad(locality)	UTF8 <Dirección física del PSC>	
Estado(state)	UTF8 <Estado en el cual se ubica el PSC>	
País(country)	UTF8 [VE] (ISO 3166-1-alpha-2)	
Información de Clave Pública del Titular		
Algoritmo de clave pública (algorithm)	<Algoritmo Asignado> (rsaEncryption, dhpublicnumber, id-dsa,)	
Clave Pública de Titular (subjectPublicKey)		
Módulo(modulus) *	Cadena de Octetos [4096 bit]	
Exponente(exponent) *	Entero Hexadecimal [65537] <0x10001>	
* Para caso de RSA se exigen estos campos		
Extensiones		
Restricciones Básicas (basicConstraints)		X
Autoridad de Certificación(aC)	Booleano [true]	
Longitud de Certificación(pathLen)	Entero Hexadecimal [0] (No permite la creación de AC en niveles inferiores a ella)	
Claves de Usos(keyUsage)		X
Firma de certificado	keyCertSign(5)	
Firma de LCR	cRLSign (6)	
Identificador de clave de Titular (Subject Key Identifier)	Valor hexadecimal <Hash> (Resultado de Función Hash)	
Nombre Alternativo del Emisor (issuerAltName)		
Otro Nombre (otherName)	<RIF del PSC>	
Identificador de clave de Autoridad Certificadora (Authority Key Identifier)		
Clave de Autoridad(keyIdentifier)	KeyIdentifier <Identificador de la clave pública de la AC Raíz>	
Nombre distintivo (authorityCertIssuer)	GeneralNames <Contiene la información de la AC Raíz con el formato DN>	
Serial (authorityCertSerialNumber)	CertificateSerialNumber <Contiene el número del certificado del emisor>	
Nombre Alternativo del Titular (subjectAltName)		
Nombre DNS (dNSName)	<DNS del Ente poseedor de la AC Subordinada >	
Otro Nombre (otherName)	<Código de identificación del PSC acreditado asignado por SUSCERTE>	
Otro Nombre (otherName)	<RIF del Ente poseedor de la AC Subordinada>	
Puntos de Distribución de las LCR (cRLDistributionPoints)		
Punto de distribución LCR (distributionPoint)	<Dirección de descarga de la LCR por el PSC>	
Puntos de Distribución de las LCR (cRLDistributionPoints)		
AIA (authorityInfoAccess)		
Método de Acceso (accessMethod)	1.3.6.1.5.5.7.48.1 [OCSP]	
Dirección de Acceso (accessLocation)	<Dirección de consulta de certificados revocados>	
Políticas de Certificación (PolicyInformation)		
PolicyInformation (PC)		
policyIdentifier	<OID Autorizado por SUSCERTE>	
cPSuri	<Dirección dónde se puede descargar la PC>	
userNotice	(No se usa)	
PolicyInformation (DPC)		
policyIdentifier	<OID Autorizado por SUSCERTE>	
cPSuri	<Dirección dónde se puede descargar la DPC>	
userNotice	(No se usa)	
Firma		
Algoritmo de Firma (signatureAlgorithm)	Algoritmo Autorizado (OID de los algoritmos permitidos mínimo SHA256withRSAEncryption o SHA384withRSAEncryption o Superior)	
Firma(signature)	<Contenido de la Firma>	

4.10.4 Estructura Certificado Persona Natural

Certificado cuyo suscriptor y titular es una persona natural, destinado para firmar electrónicamente mensajes de datos para expresar la voluntad del signatario como persona natural. Se pueden obtener diversas aplicaciones utilizando combinación de Claves de Usos y Claves de Usos Extendidos.

Certificado de Persona Natural		
Nombre(X.509)	**Tipo de dato [Constante] < Valor >**	**Crítica (para extensiones)**
Datos de Certificado		
Versión (version)	Entero Hexadecimal [V3] < 0x2 >(Representa la versión 3 del X.509)	
Serial (serialNumber)	Entero Hexadecimal<Asignado por la AC> (No negativo)	
Algoritmo de Firma (signature)	Algoritmo Autorizado	
Datos del Emisor (issuer)		
Nombre Común (commonName)	UTF8 <Identificación de la AC>	
Correo Electrónico(emailAddress)	UTF8 <Dirección de correo electrónico de contacto del Emisor>	
Teléfono (telephoneNumber)	UTF8 <Teléfono de contacto del Emisor> (Opcional)	
Departamento (organizationUnity)	UTF8 <Nombre o Razón social como aparece en documento constitutivo del PSC>	
Organización (organization)	UTF8 [Sistema Nacional de Certificación Electrónica]	
Localidad(locality)	UTF8 <Ciudad de ubicación del Emisor>	
Estado(state)	UTF8 <Estado de ubicación del Emisor>	
País(country)	UTF8 [VE] (ISO 3166-1-alpha-2)	

Datos de Validez		
No Antes(notBefore)	Fecha (UTC)	
No Después(noAfter)	Fecha (UTC)	
Datos de Titular (subject)		
Serial (serialNumber)	UTF8 <Cédula, RIF o Pasaporte>(Ver Anexo A)	
Nombre Común (commonName)	UTF8 <Nombre1 Nombre2 Apellido1 Apellido2>	
Nombre (givenName)	UTF8 <Nombre 1>(Opcional)	
Apellido (surName)	UTF8 <Apellido 1>(Opcional)	
Correo Electrónico(emailAddress)	UTF8 <Dirección de correo electrónico de contacto del Titular>	
Teléfono (telephoneNumber)	UTF8 <Número telefónico de contacto del Titular>(Opcional)	
Código Postal (postalCode)	UTF8 <Código postal al que pertenece su dirección>(Opcional)	
Calle (streetAddress)	UTF8 <Calle de residencia del Titular >(Opcional)	
Localidad(locality)	UTF8<Ciudad de residencia del Titular>	
Estado(state)	UTF8 <Estado de ubicación del Titular>	
País(country)	UTF8 [VE] (ISO 3166-1-alpha-2)	
Información de Clave Pública del Titular		
Algoritmo de clave pública (algorithm)	<Algoritmo Asignado> (rsaEncryption, dhpublicnumber, id-dsa,)	
Clave Pública de Titular (subjectPublicKey)		
Módulo(modulus) *	Cadena de Octetos [2048bit]	
Exponente(exponent) *	Entero Hexadecimal [65537] <0x10001>	
* Para caso de RSA se exigen estos campos		
Extensiones		
Restricciones Básicas (basicConstraints)		X
Autoridad de Certificación(aC)	Booleano <false>(Determina no emitir o firmar certificados)	
Claves de Usos(keyUsage)		X
Firma Digital	digitalSignature(0)	
Compromiso con el Contenido (Anteriormente No Repudio)	contentCommitment(1)	
Solo cifrado	encipherOnly(7)	
Solo descifrado	decipherOnly(8)	
** Se deben evaluar la aplicación de cada uno de estas Clave de Uso		
Usos Extendidos de la Clave(extKeyUsage)		
Firma de Código	codeSigning 1.3.6.1.5.5.7.3.3	
Protección Correo Electrónico	emailProtection 1.3.6.1.5.5.7.3.4	
Microsoft Smart Card Logon	smartCardLogon 1.3.6.1.4.1.311.20.2.2	
Microsoft Document Signing	documentSigning 1.3.6.1.4.1.311.10.3.12	
Microsoft Individual Code Signing	individualCodeSigning 1.3.6.1.4.1.311.2.1.21	
Adobe PDF Signing	adobePdfSigning 1.2.840.113583.1.1.5	
*** Los Usos Extendidos son opcionales y aplicables de acuerdo a las necesidades del Usuario		
Nombre Alternativo del Emisor (issuerAltName)		
Otro Nombre (otherName)	<RIF del PSC>	
Otro Nombre (otherName)	<Código de identificación del PSC acreditado asignado por SUSCERTE>	
Nombre DNS (dNSName)	<DNS del PSC emisor del certificado>	
Punto de distribución LCR (distributionPoint)	<LCR del repositorio del PSC>	
Identificador de clave de Autoridad Certificadora (Authority Key Identifier)		
Clave de Autoridad(keyIdentifier)	KeyIdentifier <Identificador de la clave pública de la AC Raíz>	
Nombre distintivo (authorityCertIssuer)	GeneralNames <Contiene la información de la AC Raíz con el formato DN>	
Serial (authorityCertSerialNumber)	CertificateSerialNumber <Contiene el número del certificado del emisor>	
Identificador de clave de Titular (Subject Key Identifier)	Valor hexadecimal <Hash> (Resultado de Función Hash)	
Nombre Alternativo del Titular (subjectAltName)		
Nombre RFC822 (rfc822Name)	<Correo electrónico del Titular>	
AIA (authorityInfoAccess)		
Método de Acceso (accessMethod)	1.3.6.1.5.5.7.48.1 [OCSP]	
Dirección de Acceso (accessLocation)	<URL del servicio OSCP>	
Puntos de Distribución de las LCR (cRLDistributionPoints)		
Punto de distribución LCR (distributionPoint)	<LCR del repositorio del PSC>	
Políticas de Certificación (PolicyInformation)		
PolicyInformation (PC)		
policyIdentifier	<OID Autorizado por SUSCERTE>	
cPSuri	<Dirección dónde se puede descargar la PC>	
userNotice	(No se usa)	
PolicyInformation (DPC)		
policyIdentifier	<OID Autorizado por SUSCERTE>	
cPSuri	<Dirección dónde se puede descargar la DPC>	
userNotice		
Firma		
Algoritmo de Firma (signatureAlgorithm)	Algoritmo Autorizado (OID de los algoritmos permitidos mínimo SHA256withRSAEncryption o SHA384withRSAEncryption o Superior)	
Firma(signature)	<Contenido de la Firma>	

4.10.5 Estructura Certificado Persona Jurídica

Certificado cuyo suscriptor es una empresa u organización y el titular es una persona natural que representa legalmente a dicho ente destinado para firmar electrónicamente documentos, mensajes de datos para expresar la voluntad del signatario. Se pueden obtener diversas aplicaciones utilizando combinación de Claves de Usos y Claves de Usos Extendidos.

Certificado de Persona Jurídica		
Nombre(X.509)	**Tipo de dato [Constante] < Valor >**	**Crítica (para extensiones)**
Datos de Certificado		
Versión (version)	Entero Hexadecimal [V3] < 0x2 >(Representa la versión 3 del X.509)	
Serial (serialNumber)	Entero Hexadecimal<Asignado por la AC> (No negativo)	
Algoritmo de Firma (signature)	Algoritmo Autorizado	
Datos del Emisor (issuer)		
Nombre Común (commonName)	UTF8 <Identificación de la AC>	
Correo Electrónico(emailAddress)	UTF8 <Dirección de correo electrónico de contacto del Emisor>	
Teléfono (telephoneNumber)	UTF8 <Teléfono de contacto del Emisor>	
Departamento (organizationUnity)	UTF8 <Nombre o Razón social como aparece en documento constitutivo del PSC>	
Organización (organization)	UTF8 [Sistema Nacional de Certificación Electrónica]	
Localidad(locality)	UTF8 <Ciudad de ubicación del Emisor>	
Estado(state)	UTF8 <Estado de ubicación del Emisor>	
País(country)	UTF8 [VE] (ISO 3166-1-alpha-2)	
Datos de Validez		
No Antes(notBefore)	Fecha (UTC)	
No Después(noAfter)	Fecha (UTC)	
Datos de Titular (subject)		
Serial (serialNumber)	UTF8 <Cédula, RIF o Pasaporte>(Ver Anexo A)	
Nombre Común (commonName)	UTF8 <Nombre1 Nombre2 Apellido1 Apellido2>	
Nombre (givenName)	UTF8 <Nombre 1>(Opcional)	
Apellido (surName)	UTF8 <Apellido 1>(Opcional)	
Correo Electrónico(emailAddress)	UTF8 <Dirección de correo electrónico de contacto del Titular>	
Teléfono (telephoneNumber)	UTF8 <Número telefónico de contacto del Titular>(Opcional)	
Organización (organization)	UTF8<Nombre completo de la persona jurídica o suscriptor tal cual aparece en el documento constitutivo de la organización>	
Código Postal (postalCode)	UTF8 <Código postal al que pertenece su dirección>(Opcional)	
Calle (streetAddress)	UTF8 <Calle de residencia del titular >(Opcional)	
Localidad(locality)	UTF8<Ciudad de residencia del titular>	
Estado(state)	UTF8 <Estado de ubicación del Titular>	
País(country)	UTF8 [VE] (ISO 3166-1-alpha-2)	
Información de Clave Pública del Titular		
Algoritmo de clave pública (algorithm)	<Algoritmo Asignado> (rsaEncryption, dhpublicnumber, id-dsa,)	
Clave Pública de Titular (subjectPublicKey)		
Módulo(modulus) *	Cadena de Octetos [2048bit]	
Exponente(exponent) *	Entero Hexadecimal [65537] <0x10001>	
* Para caso de RSA se exigen estos campos		
Extensiones		
Restricciones Básicas (basicConstraints)		X
Autoridad de Certificación(aC)	Booleano <false>(Determina no emitir o firmar certificados)	
Claves de Usos(keyUsage)		X
Firma Digital	digitalSignature(0)	
Compromiso con el Contenido (Anteriormente No Repudio)	contentCommitment(1)	
Solo cifrado	encipherOnly(7)	
Solo descifrado	decipherOnly(8)	
** Se deben evaluar la aplicación de cada uno de estas Clave de Uso		
Usos Extendidos de la Clave (extKeyUsage)		
Firma de Código	codeSigning 1.3.6.1.5.5.7.3.3	
Protección Correo Electrónico	emailProtection 1.3.6.1.5.5.7.3.4	
Microsoft Smart Card Logon	smartCardLogon 1.3.6.1.4.1.311.20.2.2	
Microsoft Document Signing	documentSigning 1.3.6.1.4.1.311.10.3.12	
Microsoft Comercial Code Signing	comercialCodeSingning 1.3.6.1.4.1.311.2.1.22	
Adobe PDF Signing	adobePdfSigning 1.2.840.113583.1.1.5	
*** Los Usos Extendidos son opcionales y aplicables de acuerdo a las necesidades del Usuario		
Nombre Alternativo del Emisor (issuerAltName)		
Otro Nombre (otherName)	<RIF del PSC>	
Otro Nombre (otherName)	<Código de identificación del PSC acreditado asignado por SUSCERTE>	
Nombre DNS (dNSName)	<DNS del PSC emisor del certificado>	
Identificador de clave de Autoridad Certificadora (Authority Key Identifier)		
Identificador de clave de Titular (Subject Key Identifier)	Valor hexadecimal <Hash> (Resultado de Función Hash)	
Clave de Autoridad(keyIdentifier)	KeyIdentifier <Identificador de la clave pública de la AC Raíz>	
Nombre distintivo (authorityCertIssuer)	GeneralNames <Contiene la información de la AC Raíz con el formato DN>	
Serial (authorityCertSerialNumber)	CertificateSerialNumber <Contiene el número del certificado del emisor>	
Nombre Alternativo del Titular (subjectAltName)		
Nombre RFC822 (rfc822Name)	<Correo electrónico del Titular>	
AIA (authorityInfoAccess)		
Método de Acceso (accessMethod)	1.3.6.1.5.5.7.48.1 [OCSP]	
Dirección de Acceso (accessLocation)	<URL del servicio OSCP>	
Puntos de Distribución de las LCR (cRLDistributionPoints)		
Punto de distribución LCR (distributionPoint)	<LCR del repositorio del PSC>	
Políticas de Certificación (PolicyInformation)		
PolicyInformation (PC)		
policyIdentifier	<OID Autorizado por SUSCERTE>	
cPSuri	<Dirección dónde se puede descargar la PC>	
userNotice	(No se usa)	
PolicyInformation (DPC)		
policyIdentifier	<OID Autorizado por SUSCERTE>	
cPSuri	<Dirección dónde se puede descargar la DPC>	
userNotice		
Firma		
Algoritmo de Firma (signatureAlgorithm)	Algoritmo Autorizado (OID de los algoritmos permitidos mínimo SHA256withRSAEncryption o SHA384withRSAEncryption o Superior)	
Firma(signature)	<Contenido de la Firma>	

4.10.6 Estructura Certificado Profesional Titulado

Certificado cuyo suscriptor y el titular es una persona natural perteneciente a un Gremio o Colegiatura de Profesionales, se destina para firmar electrónicamente mensajes de datos para expresar la voluntad del

signatario. Se pueden obtener diversas aplicaciones utilizando combinación de Claves de Usos y Claves de Usos Extendidos.

Certificado de Profesional Titulado		
Nombre(X.509)	**Tipo de dato [Constante] < Valor >**	**Crítica (para extensiones)**
Datos de Certificado		
Versión (version)	Entero Hexadecimal [V3] < 0x2 >(Representa la versión 3 del X.509)	
Serial (serialNumber)	Entero Hexadecimal<Asignado por la AC> (No negativo)	
Algoritmo de Firma (signature)	Algoritmo Autorizado	
Datos del Emisor (issuer)		
Nombre Común (commonName)	UTF8 <Identificación de la AC>	
Correo Electrónico(emailAddress)	UTF8 <Dirección de correo electrónico de contacto del Emisor>	
Teléfono (telephoneNumber)	UTF8 <Teléfono de contacto del Emisor> (Opcional)	
Departamento (organizationUnity)	UTF8 <Nombre o Razón social como aparece en documento constitutivo del PSC>	
Organización (organization)	UTF8 [Sistema Nacional de Certificación Electrónica]	
Localidad(locality)	UTF8 <Ciudad de ubicación del Emisor>	
Estado(state)	UTF8 <Estado de ubicación del Emisor>	
País(country)	UTF8 [VE] (ISO 3166-1-alpha-2)	
Datos de Validez		
No Antes(notBefore)	Fecha (UTC)	
No Después(noAfter)	Fecha (UTC)	
Datos de Titular (subject)		
Serial (serialNumber)	UTF8 <Cédula, RIF, Pasaporte>(Ver Anexo A)	
Nombre Común (commonName)	UTF8 <Cadena compuesta por el nombre del Profesional y el número de Colegiado>	
Nombre (givenName)	UTF8 <Nombre 1 Nombre 2> (Opcional)	
Apellido (surName)	UTF8 <Apellido 1 Apellido 2> (Opcional)	
Título (title)	UTF8 <Nombre del Título registrado ante la Colegiatura> (Opcional)	
Correo Electrónico(emailAddress)	UTF8 <Dirección de correo electrónico de contacto del Titular>	
Teléfono (telephoneNumber)	UTF8 <Número telefónico de contacto del Titular> (Opcional)	
Organización (organization)	UTF8<Nombre del Colegio al que pertenece la Colegiatura> (Opcional)	
Localidad(locality)	UTF8<Ciudad de ubicación del Titular>	
Estado(state)	UTF8 <Estado de ubicación del Titular>	
País(country)	UTF8 [VE] (ISO 3166-1-alpha-2)	
Información de Clave Pública del Titular		
Algoritmo de clave pública (algorithm)	<Algoritmo Asignado> (rsaEncryption, dhpublicnumber, id-dsa,)	
Clave Pública de Titular (subjectPublicKey)		
Módulo(modulus) *	Cadena de Octetos [2048bit]	
Exponente(exponent) *	Entero Hexadecimal [65537] <0x10001>	
* Para caso de RSA se exigen estos campos		
Extensiones		
Restricciones Básicas (basicConstraints)		X
Autoridad de Certificación(aC)	Booleano <false>(Determina no emitir o firmar certificados)	
Claves de Usos(keyUsage)		X
Firma Digital	digitalSignature(0)	
Compromiso con el Contenido (Anteriormente No Repudio)	contentCommitment(1)	
Solo cifrado	encipherOnly(7)	
Solo descifrado	decipherOnly(8)	
** Se deben evaluar la aplicación de cada uno de estas Clave de Uso		
Usos Extendidos de la Clave (extKeyUsage)		
Firma de Código	codeSigning 1.3.6.1.5.5.7.3.3	
Protección Correo Electrónico	emailProtection 1.3.6.1.5.5.7.3.4	
Microsoft Smart Card Logon	smartCardLogon 1.3.6.1.4.1.311.20.2.2	
Microsoft Document Signing	documentSigning 1.3.6.1.4.1.311.10.3.12	
Microsoft Individual Code Signing	individualCodeSigning 1.3.6.1.4.1.311.2.1.21	
Adobe PDF Signing	adobePdfSigning 1.2.840.113583.1.1.5	
*** Los Usos Extendidos son opcionales y aplicables de acuerdo a las necesidades del Usuario		
Nombre Alternativo del Emisor (issuerAltName)		
Otro Nombre (otherName)	<RIF del PSC>	
Otro Nombre (otherName)	<Código de identificación del PSC acreditado asignado por SUSCERTE>	
Nombre DNS (dNSName)	<DNS del PSC emisor del certificado>	
Identificador de clave de Autoridad Certificadora (Authority Key Identifier)		
Identificador de clave de Titular (Subject Key Identifier)	Valor hexadecimal <Hash> (Resultado de Función Hash)	
Clave de Autoridad(keyIdentifier)	KeyIdentifier <Identificador de la clave pública de la AC Raíz>	
Nombre distintivo (authorityCertIssuer)	GeneralNames <Contiene la información de la AC Raíz con el formato DN>	
Serial (authorityCertSerialNumber)	CertificateSerialNumber <Contiene el número del certificado del emisor>	
Nombre Alternativo del Titular (subjectAltName)		
Nombre RFC822 (rfc822Name)	<Correo electrónico del Titular>	
AIA (authorityInfoAccess)		
Método de Acceso (accessMethod)	1.3.6.1.5.5.7.48.1 [OCSP]	
Dirección de Acceso (accessLocation)	<URL del servicio OSCP>	
Puntos de Distribución de las LCR (cRLDistributionPoints)		
Punto de distribución LCR (distributionPoint)	<LCR del repositorio del PSC>	
Políticas de Certificación (PolicyInformation)		
PolicyInformation (PC)		
policyIdentifier	<OID Autorizado por SUSCERTE>	
cPSuri	<Dirección dónde se puede descargar la PC>	
userNotice	(No se usa)	
PolicyInformation (DPC)		
policyIdentifier	<OID Autorizado por SUSCERTE>	
cPSuri	<Dirección dónde se puede descargar la DPC>	
userNotice		
Firma		
Algoritmo de Firma (signatureAlgorithm)	Algoritmo Autorizado (OID de los algoritmos permitidos mínimo SHA256withRSAEncryption o SHA384withRSAEncryption o Superior)	
Firma(signature)	<Contenido de la Firma>	

4.10.7 Estructura Certificado Empleado de Institución Pública

Certificado cuyo suscriptor es una organización o ente del Estado y el titular o signatario es una persona natural que desempeña actividades bajo relación laboral para una institución pública. Dicho certificado se destina para firmar electrónicamente mensajes de datos para expresar la voluntad del signatario. Se pueden obtener diversas aplicaciones utilizando combinación de Claves de Usos y Claves de Usos Extendidos.

Certificado de Empleado de Institución Pública		
Nombre(X.509)	**Tipo de dato [Constante] < Valor >**	**Crítica (para extensiones)**
Datos de Certificado		
Versión (version)	Entero Hexadecimal [V3] < 0x2 >(Representa la versión 3 del X.509)	
Serial (serialNumber)	Entero Hexadecimal<Asignado por la AC> (No negativo)	
Algoritmo de Firma (signature)	Algoritmo Autorizado	
Datos del Emisor (issuer)		
Nombre Común (commonName)	UTF8 <Identificación de la AC>	
Correo Electrónico(emailAddress)	UTF8 <Dirección de correo electrónico de contacto del Emisor>	
Teléfono (telephoneNumber)	UTF8 <Teléfono de contacto del Emisor>(Opcional)	
Departamento (organizationUnity)	UTF8 <Nombre o Razón social como aparece en documento constitutivo del PSC>	
Organización (organization)	UTF8 [Sistema Nacional de Certificación Electrónica]	
Localidad(locality)	UTF8 <Ciudad de ubicación del Emisor>	
Estado(state)	UTF8 <Estado de ubicación del Emisor>	
País(country)	UTF8 [VE] (ISO 3166-1-alpha-2)	
Datos de Validez		
No Antes(notBefore)	Fecha (UTC)	
No Después(noAfter)	Fecha (UTC)	
Datos de Titular (subject)		
Serial (serialNumber)	UTF8 <Cédula, RIF, Pasaporte>(Ver Anexo A)	
Título (title)	UTF8 <Título y/o cargo o funciones del titular del certificado>	
Nombre Común (commonName)	UTF8 <Nombre1 Nombre2 Apellido1 Apellido2>	
Nombre (givenName)	UTF8 <Nombre 1> (Opcional)	
Apellido (surName)	UTF8 <Apellido 1> (Opcional)	
Identificador de documento o Nombramiento (documentIdentifier)	UTF8 <Especificar documento que lo acredita como empleado>	
Correo Electrónico(emailAddress)	UTF8 <Dirección de correo electrónico de contacto del Titular>	
Teléfono (telephoneNumber)	UTF8 <Número telefónico de contacto del Titular> (Opcional)	
Departamento (organizationUnity)	UTF8<Nombre del departamento, dirección o unidad de trabajo al cuál pertenece el titular> (Opcional)	
Organización (organization)	UTF8<Nombre completo de la persona jurídica tal cual aparece en el documento constitutivo de la organización>	
Localidad(locality)	UTF8<Ciudad donde se ubica organización propietaria del certificado>	
Estado(state)	UTF8 <Estado donde se ubica organización propietaria del certificado>	
País(country)	UTF8 [VE] (ISO 3166-1-alpha-2)	
Información de Clave Pública del Titular		
Algoritmo de clave pública (algorithm)	<Algoritmo Asignado> (rsaEncryption, dhpublicnumber, id-dsa,)	
Clave Pública de Titular (subjectPublicKey)		
Módulo(modulus) *	Cadena de Octetos [2048bit]	
Exponente(exponent) *	Entero Hexadecimal [65537] <0x10001>	
* Para caso de RSA se exigen estos campos		
Extensiones		
Restricciones Básicas (basicConstraints)		X
Autoridad de Certificación(aC)	Booleano <false>(Determina no emitir o firmar certificados)	
Claves de Usos(keyUsage)		X
Firma Digital	digitalSignature(0)	
Compromiso con el Contenido (Anteriormente No Repudio)	contentCommitment(1)	
Solo cifrado	encipherOnly(7)	
Solo descifrado	decipherOnly(8)	
** Se deben evaluar la aplicación de cada uno de estas Clave de Uso		
Usos Extendidos de la Clave (extKeyUsage)		
Firma de Código	codeSigning 1.3.6.1.5.5.7.3.3	
Protección Correo Electrónico	emailProtection 1.3.6.1.5.5.7.3.4	
Microsoft Smart Card Logon	smartCardLogon 1.3.6.1.4.1.311.20.2.2	
Microsoft Document Signing	documentSigning 1.3.6.1.4.1.311.10.3.12	
Microsoft Comercial Code Signing	comercialCodeSingning 1.3.6.1.4.1.311.2.1.22	
Adobe PDF Signing	adobePdfSigning 1.2.840.113583.1.1.5	
*** Los Usos Extendidos son opcionales y aplicables de acuerdo a las necesidades del Usuario		
Nombre Alternativo del Emisor (issuerAltName)		
Otro Nombre (otherName)	<RIF del PSC>	
Otro Nombre (otherName)	<Código de identificación del PSC acreditado asignado por SUSCERTE>	
Nombre DNS (dNSName)	<DNS del PSC emisor del certificado>	
Identificador de clave de Autoridad Certificadora (Authority Key Identifier)		
Identificador de clave de Titular (Subject Key Identifier)	Valor hexadecimal <Hash> (Resultado de Función Hash)	
Clave de Autoridad(keyIdentifier)	KeyIdentifier <Identificador de la clave pública de la AC Raíz>	
Nombre distintivo (authorityCertIssuer)	GeneralNames <Contiene la información de la AC Raíz con el formato DN>	
Serial (authorityCertSerialNumber)	CertificateSerialNumber <Contiene el número del certificado del emisor>	
Nombre Alternativo del Titular (subjectAltName)		
Otro Nombre (otherName)	<RIF del Ente Suscriptor>	
Nombre RFC822 (rfc822Name)	<Correo electrónico del Ente Suscriptor>	

AIA (authorityInfoAccess)		
Método de Acceso (accessMethod)	1.3.6.1.5.5.7.48.1 [OCSP]	
Dirección de Acceso (accessLocation)	<URL del servicio OSCP>	
Puntos de Distribución de las LCR (cRLDistributionPoints)		
Punto de distribución LCR (distributionPoint)	<LCR del repositorio del PSC>	
Políticas de Certificación (PolicyInformation)		
PolicyInformation (PC)		
policyIdentifier	<OID Autorizado por SUSCERTE>	
cPSuri	<Dirección dónde se puede descargar la PC>	
userNotice	(No se usa)	
PolicyInformation (DPC)		
policyIdentifier	<OID Autorizado por SUSCERTE>	
cPSuri	<Dirección dónde se puede descargar la DPC>	
userNotice		
Firma		
Algoritmo de Firma (signatureAlgorithm)	Algoritmo Autorizado (OID de los algoritmos permitidos mínimo SHA256withRSAEncryption o SHA384withRSAEncryption o Superior)	
Firma(signature)	<Contenido de la Firma>	

4.10.8 Estructura Certificado de Empleado de Empresa

Certificado cuyo suscriptor es una empresa u organización y el titular o signatario es una persona natural que está bajo relación laboral con dicho ente. Este certificado se destina para firmar electrónicamente documentos, mensajes de datos para expresar la voluntad del signatario. Se pueden obtener diversas aplicaciones utilizando combinación de Claves de Usos y Claves de Usos Extendidos.

Certificado de Empleado de Empresa Privada		
Nombre(X.509)	**Tipo de dato [Constante] < Valor >**	**Crítica (para extensiones)**
Datos de Certificado		
Versión (version)	Entero Hexadecimal [V3] < 0x2 >(Representa la versión 3 del X.509)	
Serial (serialNumber)	Entero Hexadecimal<Asignado por la AC> (No negativo)	
Algoritmo de Firma (signature)	Algoritmo Autorizado	
Datos del Emisor (issuer)		
Nombre Común (commonName)	UTF8 <Identificación de la AC>	
Correo Electrónico(emailAddress)	UTF8 <Dirección de correo electrónico de contacto del Emisor>	
Teléfono (telephoneNumber)	UTF8 <Teléfono de contacto del Emisor> (Opcional)	
Departamento (organizationUnity)	UTF8 <Nombre o Razón social como aparece en documento constitutivo del PSC>	
Organización (organization)	UTF8 [Sistema Nacional de Certificación Electrónica]	
Localidad(locality)	UTF8 <Ciudad de ubicación del Emisor>	
Estado(state)	UTF8 <Estado de ubicación del Emisor>	
País(country)	UTF8 [VE] (ISO 3166-1-alpha-2)	
Datos de Validez		
No Antes(notBefore)	Fecha (UTC)	
No Después(noAfter)	Fecha (UTC)	
Datos de Titular (subject)		
Serial (serialNumber)	UTF8 <Cédula, RIF, Pasaporte del signatario>(Ver Anexo A)	
Título (title)	UTF8 <Título y/o Cargo del empleado>	
Nombre Común (commonName)	UTF8 <Nombre1 Nombre2 Apellido1 Apellido2>	
Nombre (givenName)	UTF8 <Nombre 1> (Opcional)	
Apellido (surName)	UTF8 <Apellido 1> (Opcional)	
Correo Electrónico(emailAddress)	UTF8 <Dirección de correo electrónico de contacto del Titular>	
Teléfono (telephoneNumber)	UTF8 <Número telefónico de contacto del Titular> (Opcional)	
Departamento (organizationUnity)	UTF8<Nombre del departamento, dirección o unidad de trabajo al cuál pertenece el titular> (Opcional)	
Organización (organization)	UTF8<Nombre completo de la persona jurídica tal cual aparece en el documento constitutivo de la empresa>	
Localidad(locality)	UTF8<Ciudad donde se ubica organización propietaria del certificado>	
Estado(state)	UTF8 <Estado donde se ubica organización suscriptora del certificado>	
País(country)	UTF8 [VE] (ISO 3166-1-alpha-2)	
Información de Clave Pública del Titular		
Algoritmo de clave pública (algorithm)	<Algoritmo Asignado> (rsaEncryption, dhpublicnumber, id-dsa,)	
Clave Pública de Titular (subjectPublicKey)		
Módulo (modulus) *	Cadena de Octetos [2048bit]	
Exponente (exponent) *	Entero Hexadecimal [65537] <0x10001>	
* Para caso de RSA se exigen estos campos		
Extensiones		
Restricciones Básicas (basicConstraints)		X
Autoridad de Certificación(aC)	Booleano <false>(Determina no emitir o firmar certificados)	
Claves de Usos (keyUsage)		X
Firma Digital	digitalSignature(0)	
Compromiso con el Contenido (Anteriormente No Repudio)	contentCommitment(1)	
Solo cifrado	encipherOnly(7)	
Solo descifrado	decipherOnly(8)	
** Se deben evaluar la aplicación de cada uno de estas Clave de Uso		
Usos Extendidos de la Clave (extKeyUsage)		
Firma de Código	codeSigning 1.3.6.1.5.5.7.3.3	
Protección Correo Electrónico	emailProtection 1.3.6.1.5.5.7.3.4	
Microsoft Smart Card Logon	smartCardLogon 1.3.6.1.4.1.311.20.2.2	
Microsoft Document Signing	documentSigning 1.3.6.1.4.1.311.10.3.12	
Microsoft Comercial Code Signing	comercialCodeSingning 1.3.6.1.4.1.311.2.1.22	
Adobe PDF Signing	adobePdfSigning 1.2.840.113583.1.1.5	
*** Los Usos Extendidos son opcionales y aplicables de acuerdo a las necesidades del Usuario		
Nombre Alternativo del Emisor (issuerAltName)		
Otro Nombre (otherName)	<RIF del PSC>	
Otro Nombre (otherName)	<Código de identificación del PSC acreditado asignado por SUSCERTE>	
Nombre DNS (dNSName)	<DNS del PSC emisor del certificado>	
Identificador de clave de Autoridad Certificadora (Authority Key Identifier)		
Identificador de clave de Titular (Subject Key Identifier)	Valor hexadecimal <Hash> (Resultado de Función Hash)	
Clave de Autoridad(keyIdentifier)	KeyIdentifier <Identificador de la clave pública de la AC Raíz>	
Nombre distintivo (authorityCertIssuer)	GeneralNames <Contiene la información de la AC Raíz con el formato DN>	
Serial (authorityCertSerialNumber)	CertificateSerialNumber <Contiene el número del certificado del emisor>	
Nombre Alternativo del Titular (subjectAltName)		
Otro Nombre (otherName)	<RIF de la Empresa Suscriptora>	
Nombre RFC822 (rfc822Name)	<Correo electrónico de la Empresa Suscriptora>	
Nombre DNS (dNSName)	<Sitio Web de la Empresa>(Opcional)	
Puntos de Distribución de las LCR (cRLDistributionPoints)		
Punto de distribución LCR (distributionPoint)	<LCR del repositorio del PSC>	
AIA (authorityInfoAccess)		
Método de Acceso (accessMethod)	1.3.6.1.5.5.7.48.1 [OCSP]	
Dirección de Acceso (accessLocation)	<URL del servicio OSCP>	
Políticas de Certificación (PolicyInformation)		
PolicyInformation (PC)		
policyIdentifier	<OID Autorizado por SUSCERTE>	
cPSuri	<Dirección dónde se puede descargar la PC>	
userNotice	(No se usa)	
PolicyInformation (DPC)		
policyIdentifier	<OID Autorizado por SUSCERTE>	
cPSuri	<Dirección dónde se puede descargar la DPC>	
userNotice		
Firma		
Algoritmo de Firma (signatureAlgorithm)	Algoritmo Autorizado (OID de los algoritmos permitidos mínimo SHA256withRSAEncryption o SHA384withRSAEncryption o Superior)	
Firma(signature)	<Contenido de la Firma>	

4.10.9 Propuesta de Estructura de Certificado para la Cédula Electrónica

Certificado cuyo suscriptor y el titular o signatario es una persona natural, destinado a identificarlo y representarlo para permitir firmar y autenticar operaciones legales ante los trámites electrónicos con el Estado y sólo podrá ser emitido por las autoridades de certificación del ente gubernamental con competencia en identificación (SAIME). Posee atributos especiales para describir detalles de titular, por ejemplo fecha y lugar de nacimiento, nacionalidad e información biométrica.

Certificado de Cédula Electrónica		
Nombre(X.509)	**Tipo de dato [Constante] < Valor >**	**Crítica (para extensiones)**
Datos de Certificado		
Versión (version)	Entero Hexadecimal [V3] < 0x2 >(Representa la versión 3 del X.509)	
Serial (serialNumber)	Entero Hexadecimal<Asignado por la AC> (No negativo)	
Algoritmo de Firma (signature)	Algoritmo Autorizado	
Datos del Emisor (issuer)		
Nombre Común (commonName)	UTF8 <Identificación de la AC>	
Correo Electrónico(emailAddress)	UTF8 <Dirección de correo electrónico de contacto del Emisor>	
Teléfono (telephoneNumber)	UTF8 <Teléfono de contacto del Emisor>(Opcional)	
Departamento (organizationUnity)	UTF8 <Nombre o Razón social como aparece en documento constitutivo del PSC>	
Organización (organization)	UTF8 [Sistema Nacional de Certificación Electrónica]	
Localidad(locality)	UTF8 <Ciudad de ubicación del Emisor>	
Estado(state)	UTF8 <Estado de ubicación del Emisor>	
País(country)	UTF8 [VE] (ISO 3166-1-alpha-2)	
Datos de Validez		
No Antes(notBefore)	Fecha (UTC)	
No Después(noAfter)	Fecha (UTC)	
Datos del Titular		
Serial (serialNumber)	UTF8 <Cédula> (Ver Anexo A)	
Nombre Común (commonName)	UTF8 <Apellido1 Apellido2, Nombre1 Nombre2>	
Nombres (givenName)	UTF8 <Nombre 1 Nombre 2> (Opcional)	
Apellidos (surName)	UTF8 <Apellido 1 Apellido 2> (Opcional)	
Correo Electrónico(emailAddress) [1]	UTF8 <Correo electrónico de la persona natural portadora del certificado> (Opcional)	
Teléfono (telephoneNumber) [1]	UTF8 <Número telefónico de contacto del Titular> (Opcional)	
Calle (streetAddress) [1]	UTF8 <Calle de residencia del Titular>(Opcional)	
Localidad(locality)	UTF8<Ciudad de residencia del Titular>	
Estado(state)	UTF8 <Estado de ubicación del Titular>	
País(country)	UTF8 [VE] (ISO 3166-1-alpha-2)	
1.- Condicionado a la capacidad del dispositivo y al marco legal de protección de datos personales.		
Información de Clave Pública del Titular		
Algoritmo de clave pública (algorithm)	<Algoritmo Asignado> (rsaEncryption, dhpublicnumber, id-dsa,)	
Clave Pública de Titular (subjectPublicKey)		
Módulo(modulus) [2]	Cadena de Octetos [2048bit]	
Exponente(exponent) [2]	Entero Hexadecimal [65537] <0x10001>	
2.- Para caso de RSA se exigen estos campos		
Extensiones		
Restricciones Básicas (basicConstraints)		X
Autoridad de Certificación(aC)	Booleano <false>(Determina no emitir o firmar certificados)	
Claves de Usos (keyUsage)		X
Firma Digital	digitalSignature(0)	
Compromiso con el Contenido (Anteriormente No Repudio)	contentCommitment(1)	
Solo cifrado	encipherOnly(7)	
Solo descifrado	decipherOnly(8)	
*Se debe evaluar la aplicación de cada uno de estos Usos		
Usos Extendidos de las Claves (extKeyUsage)		
Firma de Código	codeSigning 1.3.6.1.5.5.7.3.3	
Protección Correo Electrónico	emailProtection 1.3.6.1.5.5.7.3.4	
Microsoft Smart Card Logon	smartCardLogon 1.3.6.1.4.1.311.20.2.2	
Microsoft Document Signing	documentSigning 1.3.6.1.4.1.311.10.3.12	
Microsoft Individual Code Signing	individualCodeSigning 1.3.6.1.4.1.311.2.1.21	
Adobe PDF Signing	adobePdfSigning 1.2.840.113583.1.1.5	

** Los Usos Extendidos son opcionales y aplicables de acuerdo a las necesidades del Usuario		
Nombre Alternativo del Emisor (issuerAltName)		
Otro Nombre (otherName)	<RIF del PSC>	
Otro Nombre (otherName)	<Código de identificación del PSC acreditado asignado por SUSCERTE>	
Nombre DNS (dNSName)	<DNS del PSC emisor del certificado>	
Identificador de clave de Autoridad Certificadora (Authority Key Identifier)		
Identificador de clave de Titular (Subject Key Identifier)	Valor hexadecimal <Hash> (Resultado de Función Hash)	
Clave de Autoridad(keyIdentifier)	KeyIdentifier <Identificador de la clave pública de la AC Raíz>	
Nombre distintivo (authorityCertIssuer)	GeneralNames <Contiene la información de la AC Raíz con el formato DN>	
Serial (authorityCertSerialNumber)	CertificateSerialNumber <Contiene el número del certificado del emisor>	
Atributos Adicionales del Titular (subjectDirectoryAttributes)		
Atributos o Características del titular (Attributes) Crítico		X
Fecha de Nacimiento (dateOfBirth)	<Fecha de Nacimiento del Titular> (Datos visibles en la tarjeta criptográfica)	
Lugar de Nacimiento (placeOfBirth)	<Lugar de Nacimiento del Titular> (Ver Anexo H, Datos visibles en la tarjeta criptográfica)	
Género (gender)	<Género del Titular> (Ver Anexo H)	
País de Ciudadanía (countryOfCitizenship)	<País de Ciudadanía del Titular> (Formato UTF8 ISO 3166-1-alpha-2, Datos visibles en la tarjeta criptográfica)	
País de Residencia (countryOfResidence)	<País de Residencia del Titular> (Formato UTF8 ISO 3166-1-alpha-2, Datos visibles en la tarjeta criptográfica)	
Información Biométrica (biometricInfo)		
Tipo de datos biométrico (typeOfBiometricData)	<Tipo de información biométrica que hace referencia esta extensión>	
Algoritmo de Hash (hashAlgorithm)	<Es la función hash utilizada>	
Hash de datos Biométricos (biometricDataHash)	Es el resultado de la función hash de la información biométrica.	
URI de la Fuente (sourceDataUri)	<Contiene la ubicación de dónde se almacena la información biométrica>	
Puntos de Distribución de las LCR (cRLDistributionPoints)		
Punto de distribución LCR (distributionPoint)	<LCR del repositorio del PSC>	
AIA (authorityInfoAccess)		
Método de Acceso (accessMethod)	1.3.6.1.5.5.7.48.1 [OCSP]	
Dirección de Acceso (accessLocation)	<URL del servicio OSCP>	
Políticas de Certificación (PolicyInformation)		
PolicyInformation (PC)		
policyIdentifier	<OID Autorizado por SUSCERTE>	
cPSuri	<Dirección dónde se puede descargar la PC>	
userNotice	(No se usa)	
PolicyInformation (DPC)		
policyIdentifier	<OID Autorizado por SUSCERTE>	
cPSuri	<Dirección dónde se puede descargar la DPC>	
userNotice		
Firma		
Algoritmo de Firma (signatureAlgorithm)	Algoritmo Autorizado (OID de los algoritmos permitidos mínimo SHA256withRSAEncryption o SHA384withRSAEncryption o Superior)	
Firma(signature)	<Contenido de la Firma>	

4.10.10 Estructura Certificado de Servidor

Certificado cuyo suscriptor es una persona natural o jurídica y cuyo principal objetivo es identificar a un servicio web y proporcionarle seguridad a la comunicación. Entre las aplicaciones que se le puede dar a este tipo certificado está la de Servidor SSL/TLS, Servidor SSL/TLS con Validación Extendida, Servidor de Conexiones VPN, Servidor de Correo Electrónico, entre otras aplicaciones, se pueden hacer implementaciones más específicas agregando Claves de Usos y Claves Usos Extendidos.

Certificado de Servidor (General)		
Nombre(X.509)	**Tipo de dato [Constante] < Valor >**	**Crítica (para extensiones)**
Datos de Certificado		
Versión (version)	Entero Hexadecimal [V3] < 0x2 >(Representa la versión 3 del X.509)	
Serial (serialNumber)	Entero Hexadecimal<Asignado por la AC> (No negativo)	
Algoritmo de Firma (signature)	Algoritmo Autorizado	
Datos del Emisor (issuer)		
Nombre Común (commonName)	UTF8 <Identificación de la AC>	
Correo Electrónico(emailAddress)	UTF8 <Dirección de correo electrónico de contacto del Emisor>	
Teléfono (telephoneNumber)	UTF8 <Teléfono de contacto del Emisor>(Opcional)	
Departamento (organizationUnity)	UTF8 <Nombre o Razón social como aparece en documento constitutivo del PSC>	
Organización (organization)	UTF8 [Sistema Nacional de Certificación Electrónica]	
Localidad(locality)	UTF8 <Ciudad de ubicación del Emisor>	
Estado(state)	UTF8 <Estado de ubicación del Emisor>	
País(country)	UTF8 [VE] (ISO 3166-1-alpha-2)	
Datos de Validez		
No Antes(notBefore)	Fecha (UTC)	
No Después(noAfter)	Fecha (UTC)	
Datos del Titular		
Nombre Común (commonName)	UTF8 <Identificación del servidor, dominio o la aplicación>	
Serial (serialNumber)	UTF8 <RIF de la organización o empresa suscriptora del certificado>	
Correo Electrónico(emailAddress)	UTF8 <Correo electrónico de la Organización suscriptora>	
Teléfono (telephoneNumber)	UTF8 <Número telefónico del departamento que se encarga de la administración y/o seguridad del servidor> (Opcional)	
Departamento (organizationUnity)	UTF8<Nombre del departamento, dirección o unidad de trabajo al cuál pertenece el titular> (Opcional)	
Organización (organization)	UTF8<Nombre completo de la persona jurídica tal cual aparece en el documento constitutivo de la empresa suscriptora>	
Categoría de Negocio (businessCategory)*	UTF8<"Private Organization" || " Government Entity" || " Business Entity" || "Non-Commercial Entity">(Sólo una de las siguientes opciones)	
País de Jurisdicción (jurisdictionCountryName)*	UTF8 [VE] (ISO 3166-1-alpha-2, Aplica para Certificados de Validación Extendida)	
Código Postal (postalCode)	UTF8 <Código Postal donde se ubica la organización propietaria del certificado>(Opcional)	
Calle (streetAddress)	UTF8 <Dirección donde se ubica organización propietaria del certificado>(Opcional)	
Localidad(locality)	UTF8<Ciudad donde se ubica organización propietaria del certificado>	
Estado(state)	UTF8 <Estado donde se ubica organización suscriptora del certificado>	
País(country)	UTF8 [VE] (ISO 3166-1-alpha-2)	
* Necesarios para la Certificación EV		
Información de Clave Pública del Titular		
Algoritmo de clave pública (algorithm)	<Algoritmo Asignado> (rsaEncryption, dhpublicnumber, id-dsa,)	
Clave Pública de Titular (subjectPublicKey)		
Módulo(modulus) *	Cadena de Octetos [2048bit]	
Exponente(exponent) *	Entero Hexadecimal [65537] <0x10001>	
* Para caso de RSA se exigen estos campos		
Extensiones		
Restricciones Básicas (basicConstraints)		X
Autoridad de Certificación(aC)	Booleano <false>(Determina no emitir o firmar certificados)	
Claves de Usos (keyUsage)		
Firma Digital	digitalSignature(0)	
Compromiso con el Contenido (Anteriormente No Repudio)	contentCommitment(1)	
Cifrado de claves	keyEncipherment(2)	
Acuerdo de claves	keyAgreement(4)	
** Se deben evaluar la aplicación de cada uno o combinación de estas Clave de Uso.		
Usos Extendidos de la Clave (extKeyUsage)		
Autenticación de Servidor	serverAuth 1.3.6.1.5.5.7.3.1	
*** Los Usos Extendidos son opcionales y aplicables de acuerdo a las necesidades del Usuario y deben ser sometidos a un análisis técnico de acuerdo a las necesidades (Para más información Ver Anexo E)		
Nombre Alternativo del Emisor (issuerAltName)		
Otro Nombre (otherName)	<RIF del PSC>	
Otro Nombre (otherName)	<Código de identificación del PSC acreditado asignado por SUSCERTE>	
Nombre DNS (dNSName)	<DNS del PSC emisor del certificado>	
Identificador de clave de Autoridad Certificadora (Authority Key Identifier)		
Identificador de clave de Titular (Subject Key Identifier)	Valor hexadecimal <Hash> (Resultado de Función Hash)	
Clave de Autoridad(keyIdentifier)	KeyIdentifier <Identificador de la clave pública de la AC Raíz>	
Nombre distintivo (authorityCertIssuer)	GeneralNames <Contiene la información de la AC Raíz con el formato DN>	
Serial (authorityCertSerialNumber)	CertificateSerialNumber <Contiene el número del certificado del emisor>	
Nombre Alternativo del Titular (subjectAltName)		
Otro Nombre (otherName)	<RIF de la Empresa Suscriptora>	
Nombre RFC822 (rfc822Name)	<Correo electrónico de la Empresa Suscriptora>	
Nombre DNS (dNSName)	<Sitio Web de la Empresa> (Mínimo debe colocarse un DNS, se pueden agregar todos los que posea la empresa de acuerdo a la política del certificado)	
Puntos de Distribución de las LCR (cRLDistributionPoints)		
Punto de distribución LCR (distributionPoint)	<LCR del repositorio del PSC>	
AIA (authorityInfoAccess)		
Método de Acceso (accessMethod)	1.3.6.1.5.5.7.48.1 [OCSP]	
Dirección de Acceso (accessLocation)	<URL del servicio OSCP>	
AIA (authorityInfoAccess)		
Método de Acceso (accessMethod)	1.3.6.1.5.5.7.48.2	
Dirección de Acceso (accessLocation)	<URL del certificado de la autoridad>	
Políticas de Certificación (PolicyInformation)		
PolicyInformation (PC)		
policyIdentifier	<OID Autorizado por SUSCERTE>	
cPSuri	<Dirección dónde se puede descargar la PC>	
userNotice	(No se usa)	
PolicyInformation (DPC)		
policyIdentifier	<OID Autorizado por SUSCERTE>	
cPSuri	<Dirección dónde se puede descargar la DPC>	
userNotice		
Firma		
Algoritmo de Firma (signatureAlgorithm)	Algoritmo Autorizado (OID de los algoritmos permitidos mínimo SHA256withRSAEncryption o SHA384withRSAEncryption o Superior)	
Firma(signature)	<Contenido de la Firma>	

4.10.11 Estructura Certificado de Servidor de OCSP

Emitido para Firmar respuestas generadas del servicio OCSP de una AC.

Certificado de Servidor de OCSP Responder		
Nombre(X.509)	**Tipo de dato [Constante] < Valor >**	**Crítica (para extensiones)**
Datos de Certificado		
Versión (version)	Entero Hexadecimal [V3] < 0x2 >(Representa la versión 3 del X.509)	
Serial (serialNumber)	Entero Hexadecimal<Asignado por la AC> (No negativo)	
Algoritmo de Firma (signature)	Algoritmo Autorizado	
Datos del Emisor (issuer)		
Nombre Común (commonName)	UTF8 <Identificación de la AC>	
Correo Electrónico(emailAddress)	UTF8 <Dirección de correo electrónico de contacto del Emisor>	
Teléfono (telephoneNumber)	UTF8 <Teléfono de contacto del Emisor> (Opcional)	
Departamento (organizationUnity)	UTF8 <Nombre o Razón social como aparece en documento constitutivo del PSC>	
Organización (organization)	UTF8 [Sistema Nacional de Certificación Electrónica]	
Localidad(locality)	UTF8 <Ciudad de ubicación del Emisor>	
Estado(state)	UTF8 <Estado de ubicación del Emisor>	
País(country)	UTF8 [VE] (ISO 3166-1-alpha-2)	
Datos de Validez		
No Antes(notBefore)	Fecha (UTC)	
No Después(noAfter)	Fecha (UTC)	
Datos del Titular		
Nombre Común (commonName)	UTF8 <Identificación del servidor OCSP Responder>	
Correo Electrónico(emailAddress)	UTF8 <Dirección de correo electrónico de contacto de la Unidad Responsable>	

Organización (organization)	UTF8 <Nombre o Razón social como aparece en documento constitutivo de la AC>	
Localidad(locality)	UTF8 <Ciudad de ubicación del Titular>	
Estado(state)	UTF8 <Estado de ubicación del Titular>	
País(country)	UTF8 [VE] (ISO 3166-1-alpha-2)	
Información de Clave Pública del Titular		
Algoritmo de clave pública (algorithm)	<Algoritmo Asignado> (rsaEncryption, dhpublicnumber, id-dsa,)	
Clave Pública de Titular (subjectPublicKey)		
Módulo(modulus) *	Cadena de Octetos [2048bit]	
Exponente(exponent) *	Entero Hexadecimal [65537] <0x10001>	
* Para caso de RSA se exigen estos campos		
Extensiones		
Restricciones Básicas (basicConstraints)		X
Autoridad de Certificación(aC)	Booleano <false>(Determina no emitir o firmar certificados)	
Claves de Usos (keyUsage)		
Firma Digital	digitalSignature(0)	
Compromiso con el Contenido (Anteriormente No Repudio)	contentCommitment(1)	
Cifrado de claves	keyEncipherment(2)	
Acuerdo de claves	keyAgreement(4)	
** Se deben evaluar la aplicación de cada uno o combinación de estas Clave de Uso.		
Usos Extendidos de la Clave (extKeyUsage)		
Firma de OCSP	ocspSigning 1.3.6.1.5.5.7.3.9	
*** Los Usos Extendidos son opcionales y aplicables de acuerdo a las necesidades del Usuario y deben ser sometidos a un análisis técnico de acuerdo a las necesidades (Para más información Ver Anexo E)		
Nombre Alternativo del Emisor (issuerAltName)		
Otro Nombre (otherName)	<RIF del PSC>	
Otro Nombre (otherName)	<Código de identificación del PSC acreditado asignado por SUSCERTE>	
Nombre DNS (dNSName)	<DNS del PSC emisor del certificado>	
Identificador de clave de Autoridad Certificadora (Authority Key Identifier)		
Identificador de clave de Titular (Subject Key Identifier)	Valor hexadecimal <Hash> (Resultado de Función Hash)	
Clave de Autoridad(keyIdentifier)	KeyIdentifier <Identificador de la clave pública de la AC Raíz>	
Nombre distintivo (authorityCertIssuer)	GeneralNames <Contiene la información de la AC Raíz con el formato DN>	
Serial (authorityCertSerialNumber)	CertificateSerialNumber <Contiene el número del certificado del emisor>	
Nombre Alternativo del Titular (subjectAltName)		
Nombre DNS (dNSName)	<DNS del PSC>	
Puntos de Distribución de las LCR (cRLDistributionPoints)		
Punto de distribución LCR (distributionPoint)	<LCR del repositorio del PSC>	
AIA (authorityInfoAccess)		
Método de Acceso (accessMethod)	1.3.6.1.5.5.7.48.2 [OCSP]	
Dirección de Acceso (accessLocation)	<URL del servicio OSCP>	
Políticas de Certificación (PolicyInformation)		
PolicyInformation (PC)		
policyIdentifier	<OID Autorizado por SUSCERTE>	
cPSuri	<Dirección dónde se puede descargar la PC>	
userNotice	(No se usa)	
PolicyInformation (DPC)		
policyIdentifier	<OID Autorizado por SUSCERTE>	
cPSuri	<Dirección dónde se puede descargar la DPC>	
userNotice		
Firma		
Algoritmo de Firma (signatureAlgorithm)	Algoritmo Autorizado (OID de los algoritmos permitidos mínimo SHA256withRSAEncryption o SHA384withRSAEncryption o Superior)	
Firma(signature)	<Contenido de la Firma>	

4.10.12 Estructura Certificado de Dispositivos Móviles

Destinado a mejorar la privacidad en las comunicaciones y utilización de aplicaciones seguras en Dispositivos Móviles.

Certificado de Dispositivos Móviles		
Nombre(X.509)	**Tipo de dato [Constante] < Valor >**	**Crítica (para extensiones)**
Datos de Certificado		
Versión (version)	Entero Hexadecimal [V3] < 0x2 >(Representa la versión 3 del X.509)	
Serial (serialNumber)	Entero Hexadecimal<Asignado por la AC> (No negativo)	
Algoritmo de Firma (signature)	Algoritmo Autorizado	
Datos del Emisor (issuer)		
Nombre Común	UTF8 <Identificación de la AC>	
(commonName)		
Correo Electrónico(emailAddress)	UTF8 <Dirección de correo electrónico de contacto del Emisor>	
Teléfono (telephoneNumber)	UTF8 <Teléfono de contacto del Emisor>(Opcional)	
Departamento (organizationUnity)	UTF8 <Nombre o Razón social como aparece en documento constitutivo del PSC>	
Organización (organization)	UTF8 [Sistema Nacional de Certificación Electrónica]	
Localidad(locality)	UTF8 <Ciudad de ubicación del Emisor>	
Estado(state)	UTF8 <Estado de ubicación del Emisor>	
País(country)	UTF8 [VE] (ISO 3166-1-alpha-2)	
Datos de Validez		
No Antes(notBefore)	Fecha (UTC)	
No Después(noAfter)	Fecha (UTC)	
Datos de Titular (subject)		
Nombre Común (commonName)	UTF8 <Nombre1 Nombre2 Apellido1 Apellido2>	
Serial (serialNumber)	UTF8 <IMEI del dispositivo móvil>	
Nombres (givenName)	UTF8 <Nombre 1 Nombre 2> (Opcional)	
Apellidos (surName)	UTF8 <Apellido 1 Apellido 2> (Opcional)	
Correo Electrónico(emailAddress)	UTF8 <Correo electrónico de contacto del Titular>	
Teléfono (telephoneNumber)	UTF8 <Número telefónico de contacto del Titular> (Opcional)	
Departamento (organizationUnity)	UTF8<Nombre del departamento, dirección o unidad de trabajo al cuál pertenece el titular> (Opcional)	
Organización (organization)	UTF8<Nombre completo de la persona jurídica tal cual aparece en el documento constitutivo de la empresa suscriptora> (Opcional)	
Calle (streetAddress)	UTF8 <Dirección donde se ubica el titular o suscriptor del certificado>(Opcional)	
Localidad(locality)	UTF8<Ciudad donde se ubica el titular o suscriptor del certificado>	
Estado(state)	UTF8 <Estado donde se ubica el titular o suscriptor del certificado>	
País(country)	UTF8 [VE] (ISO 3166-1-alpha-2)	
Información de Clave Pública del Titular		
Algoritmo de clave pública (algorithm)	<Algoritmo Asignado> (rsaEncryption, dhpublicnumber, id-dsa,)	
Clave Pública de Titular (subjectPublicKey)		
Módulo(modulus) *	Cadena de Octetos [2048bit]	
Exponente(exponent) *	Entero Hexadecimal [65537] <0x10001>	
* Para caso de RSA se exigen estos campos		
Extensiones		
Restricciones Básicas (basicConstraints)		X
Autoridad de Certificación(aC)	Booleano <false> (Determina no emitir o firmar certificados)	
Claves de Usos (keyUsage)		X
Firma Digital	digitalSignature(0)	
Compromiso con el Contenido (Anteriormente No Repudio)	contentCommitment(1)	
Cifrado de claves	keyEncipherment(2)	
Acuerdo de claves	keyAgreement(4)	
** Se deben evaluar la aplicación de cada uno o combinación de estas Clave de Uso.		
Usos Extendidos de la Clave (extKeyUsage)		
Autenticación de Servidor	serverAuth 1.3.6.1.5.5.7.3.1	
Autenticación de Cliente	clientAuth 1.3.6.1.5.5.7.3.2	
*** Los Usos Extendidos son opcionales y aplicables de acuerdo a las necesidades del Usuario y deben ser sometidos a un análisis técnico de acuerdo a las necesidades (Para más información Ver Anexo E)		
Identificador de clave de Titular (Subject Key Identifier)	**Valor hexadecimal <Hash> (Resultado de Función Hash)**	
Nombre Alternativo del Emisor (issuerAltName)		
Otro Nombre (otherName)	<RIF del PSC>	
Otro Nombre (otherName)	<Código de identificación del PSC acreditado asignado por SUSCERTE>	
Nombre DNS (dNSName)	<DNS del PSC emisor del certificado>	
Identificador de clave de Autoridad Certificadora (Authority Key Identifier)		
Clave de Autoridad(keyIdentifier)	KeyIdentifier <Identificador de la clave pública de la AC Raíz>	
Nombre distintivo (authorityCertIssuer)	GeneralNames <Contiene la información de la AC Raíz con el formato DN>	
Serial (authorityCertSerialNumber)	CertificateSerialNumber <Contiene el número del certificado del emisor>	
Nombre Alternativo del Titular (subjectAltName)		
Otro Nombre (otherName)	<RIF de la Empresa Suscriptora>	
Nombre RFC822 (rfc822Name)	<Correo electrónico de la Empresa Suscriptora>	
Nombre DNS (dNSName)	<Sitio Web de la Empresa> (Mínimo debe colocarse un DNS, se pueden agregar todos los que posea la empresa de acuerdo a la política del certificado)	
Puntos de Distribución de las LCR (cRLDistributionPoints)		
Punto de distribución LCR (distributionPoint	<LCR del repositorio del PSC>	
AIA (authorityInfoAccess)		
Método de Acceso (accessMethod)	1.3.6.1.5.5.7.48.1 [OCSP]	
Dirección de Acceso (accessLocation)	<URL del servicio OSCP>	
Políticas de Certificación (PolicyInformation)		
PolicyInformation (PC)		
policyIdentifier	<OID Autorizado por SUSCERTE>	
cPSuri	<Dirección dónde se puede descargar la PC>	
userNotice	(No se usa)	
PolicyInformation (DPC)		
policyIdentifier	<OID Autorizado por SUSCERTE>	
cPSuri	<Dirección dónde se puede descargar la DPC>	
userNotice		
Firma		
Algoritmo de Firma (signatureAlgorithm)	Algoritmo Autorizado (OID de los algoritmos permitidos mínimo SHA256withRSAEncryption o SHA384withRSAEncryption o Superior)	
Firma(signature)	<Contenido de la Firma>	

Artículo 3. Con la publicación en Gaceta Oficial de esta Providencia queda sin efecto la **NORMA SUSCERTE 032-01/11 edición 2 DE FECHA 30 de Enero 2011.**

Artículo 4. La Norma N° **032-06/17 " INFRAESTRUCTURA NACIONAL DE CERTIFICACIÓN ELECTRÓNICA: ESTRUCTURA, CERTIFICADOS Y LISTAS DE CERTIFICADOS REVOCADOS",** se encuentra a disposición en la sede de La Superintendencia de Servicios de Certificación Electrónica como en la página Web www.suscerte.gob.ve.

Artículo 5. La presente Providencia Administrativa entrará en vigencia a partir de su publicación en la Gaceta Oficial de la República Bolivariana de Venezuela.

Comuníquese y Publíquese.

LUIS FERNANDO PRADA FUENTES

Resolución Nº 095 del 19 de junio de 2.017, publicada en la Gaceta Oficial de la República Bolivariana de Venezuela Nº 41.177 de fecha 21 de junio de 2.017. Resolución N° 106 de fecha 13 de julio de 2.017, publicada en la Gaceta Oficial de la República Bolivariana de Venezuela N° 41.195 en fecha 18 de julio de 2.017