INFRAESTRUCTURA NACIONAL DE CERTIFICACIÓN ELECTRÓNICA:

ESTRUCTURA, CERTIFICADOS Y LISTAS DE CERTIFICADOS REVOCADOS

Firmado Por: Carlos Eduardo Parra Falcon
Fecha: 27-12-2023 16:36:41
Razón: Firma electrónica
Ubicación: Despacho del Superintendente
Contacto: Cparra@suscerte.gob.ve
SOFE Escritorio FIIIDT-CSICE

CONTROL DE VERSIONES

VERSIÓN (EDICIÓN)	MOTIVO DEL CAMBIO	PUBLICACIÓN
1.1	Creación	Abril 2008
1.2	Modificaciones en los campos: punto de distribución de CRL, acceso a la información de autoridad OCSP y Políticas del certificado.	Julio 2008
2	Clasificación de la norma	Enero 2011
3	Actualización General	Enero 2016
3.1	Firma electrónica para garantizar su integridad por las autoridades actuales	Mayo 2017
3.2	Simplificación de las tablas de certificado	Junio 2017
4	Actualización General	Diciembre 2023

ÍNDICE

TRÁMITE	
DIRECTORIO	
NOMBRE	**CARGO**
Carlos Parra	Superintendente
José Francisco Hurtado	Superintendente Adjunto
Nelly Pérez	Directora de Estandarización y Fiscalización en Certificación Electrónica y Seguridad de la Información.
	Dirección de Servicios de Certificación Electrónica y Criptografía.
Mónica Lugo	Consultora Jurídica.
EDICIÓN Y REVISIÓN	
Andrys Archila; Wainer Nelson, Nohely Coronado; Rosa María Medina; Jeison Macea; Brian Peraza.	
ASESORÍA TÉCNICA	
Alexander Osorio Delgado.	

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 Proveedores de Servicios de Certificación (PSC) acreditados ante la Superintendencia.

2. Referencias Normativas

- Constitución de la República Bolivariana de Venezuela (Febrero 2009).
- Decreto con Fuerza de Ley 1.204 Sobre Mensajes de Datos y Firmas Electrónicas (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.4 Tecnología de la Información. Sistemas abiertos Interconexión: el Directorio: Marcos para certificados de claves públicas y atributos (2019).
- RFC 5280 Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (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).
- ETSI TS 123 003 V16.3.0 Digital cellular telecommunications system (Phase 2+) (GSM); Universal Mobile Telecommunications System (UMTS); LTE; 5G; Numbering, addressing and identification (2020-10).
- RFC 3647 Public Key Infrastructure Certificate Policy and Certification Practices Framework. (2003).
- CA Browser-Forum-BR-2.0.1 Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates (08-2023).
- ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection.
- ISO/IEC 27002:2022 Information security, cybersecurity and privacy protection.

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 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	Documento mantenido y publicado por una Autoridad de Certificación

CERTIFICADOS REVOCADOS	(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.
CERTIFICADO RAÍZ	El Certificado autofirmado emitido por la AC Raíz para identificarse y facilitar la verificación de los Certificados emitidos a sus AC Subordinadas.
PC	Política de certificados es un conjunto de reglas que indica la aplicabilidad de un certificado designado a una comunidad en particular y/o implementación de PKI con requisitos de seguridad comunes.
CLAVE PÚBLICA	Sistema criptográfico que se distingue por emplear dos llaves para el intercambio de mensajes digitales. Una llave es pública y otra es privada. Una clave se designa como "pública" cuando puede ser usada por cualquier persona.
DIRECCIÓN IP	Secuencia numérica que identifica de manera única y jerárquica a cada interfaz de red, normalmente el dispositivo (computadora, portátil, teléfono inteligente) conectado a la red.
ISSUER	Es la entidad que verificó la información y firmó el certificado.
DN	Acrónimo de Distinguished Name (Nombre Distinguido) y es un conjunto de valores que se ingresa durante el proceso de inscripción y la creación de una solicitud de firma de certificado (CSR).
TOKEN CRIPTOGRÁFICO	Dispositivo criptográfico que se basa en un microprocesador que brinda soluciones para la autenticación en certificados digitales y generación de firmas digitales con valor legal.

FORMATO UTC	El Tiempo Universal Coordinado por sus siglas en ingles UTC o hora civil, que es la zona horaria de referencia a partir de la cual se calculan todas las demás partes del mundo.
MEDIA ACCESS CONTROL	Identificador único que las empresas fabricantes de hardware asignan a la tarjeta de red de cada uno de los dispositivos que producen con el fin de que sean inequívocamente identificables en sus accesos a cualquier red (lo que por supuesto incluye a Internet).
CURVA ELÍPTICA (ECDSA)	Es un enfoque de la criptografía de clave pública basado en la estructura algebraica de curvas elípticas sobre campos finitos.
LDAP	Estándar de Internet que proporciona acceso a la información desde distintas aplicaciones y sistemas informáticos. LDAP usa un conjunto de protocolos para acceder a los directorios y recuperar la información.

4. Símbolos y Abreviaturas

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

AC/CA	Autoridad de Certificación/Certification Authority.
AR/RA	Autoridad de Registro/Registration Authority.
AIA	Acceso a la Información de Autoridad
ASN.1	Abstract Syntax Notation One/Notación de Sintaxis Abstracta Uno.
DPC	Declaración de Prácticas de Certificación.
ICP/PKI	Public Key Infrastructure/ Infraestructura de clave pública
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 pre-grabado 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.
DNS	Domain Name System/Sistema de nombres de dominio.
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.
LDAP	Lightweight Directory Access Protocol, Protocolo ligero de acceso a directorios.

MAC	Media Access Control traducido en español (control de acceso al medio).

5. PROCEDIMIENTO

5.1 Principio Básico

La presente norma tiene como principio describir los aspectos técnicos de los certificados como: clasificación, valores, estructura, organización interna y especificar los requerimientos de la Infraestructura Nacional de Certificación Electrónica.

5.2 Consideraciones Generales

5.2.1 Para la selección del modelo de la Infraestructura Nacional de Certificación Electrónica, se realizó un estudio de los diferentes tipos de Infraestructura de Claves Públicas, seleccionando 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.

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

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

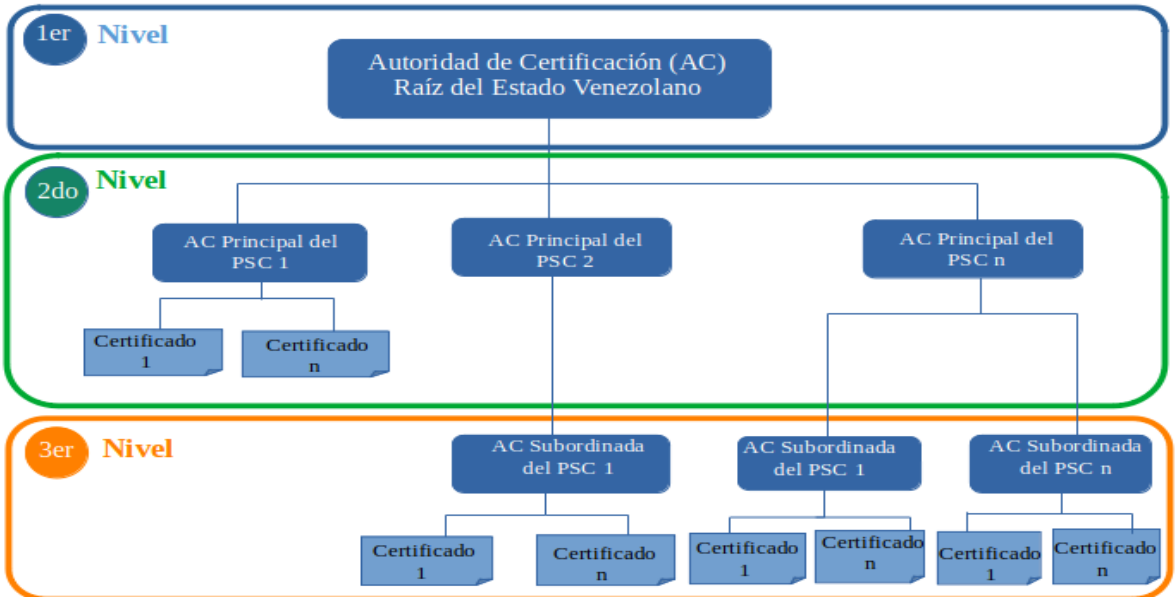

Figura Nº 1. Modelo de Jerarquía.

5.2.4 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.

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

5.2.6 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.

5.2.7 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 éstas se ve comprometida no afectará a las otras.

5.2.8 No existirá otra AC que pueda firmar el certificado AC Raíz, el único caso es cuando la AC Raíz crea el certificado autofirmado para iniciar la cadena de confianza.

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

5.2.10 La AC Raíz generará y firmará los certificados de la AC principal de los PSC.

5.2.10.1 Los PSC, a su vez, generarán y firmarán los certificados de usuarios finales o de sus AC subordinadas y éstas sólo generarán y firmarán los certificados de sus usuarios finales.

5.2.10.2 La AC raíz valida las AC subordinadas, que a su vez emiten certificados a las AC de nivel inferior o directamente a suscriptores.

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

5.3 Consideraciones Específicas

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

5.3.2 Los PSC son responsables de emitir, suspender y revocar los certificados electrónicos de sus signatarios. 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 de Ley sobre Mensajes de Datos y Firmas Electrónicas.

5.3.3 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. Deben tener condiciones especiales de generación y resguardo de los mismos, garantizando el vínculo entre la identidad de un individuo y su clave pública.

b) **Certificados para Personas**: Se generan cuando el signatario sea una persona natural ó jurídica, quien en nombre propio o representación de tercero 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: tarjeta inteligente, token USB, software, entre otros.

c) **Certificados para Sistemas**: Serán usados por componentes, equipos y/o dispositivos que requieran o no de la intervención directa de la persona.

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

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

5.3.4 Los tipos de certificados electrónicos a ser emitidos por los PSC deben cumplir con lo establecido en la presente Norma y en los estándares de la materia, y someterse a consideración, evaluación y aprobación por parte de SUSCERTE.

5.3.5 En la tabla N.º 1 se describen los tipos de certificados, los dispositivos para la generación, almacenamiento del par de claves, la vigencia y el tamaño mínimo 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)	30	521
AC Principal PSC		10 años con 3 meses	521
AC Subordinada PSC		7 años con 3 meses	521
AC Caso Especial		Depende del caso	521
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 personas naturales ó jurídicas	Software	Depende del caso	521
	Hardware (token criptográfico, tarjeta inteligente)	Depende del caso	521
Para software o aplicaciones	Software	Depende del caso	521
	Hardware (HSM)	Depende del caso	521

Tabla Nº 1.

5.3.6 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.

5.3.7 Los procedimientos para las solicitudes y emisiones de los pares de claves, se especificarán en la DPC y/o PC del PSC.

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

5.3.9 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 solicitud por parte de menores de edad, el PSC deberá evaluar legalmente, conforme lo establecido en las leyes especiales que correspondan. En el caso de extranjeros, serán identificados en el certificado electrónico con su número de pasaporte.

5.4. Procedimiento General

5.4.1 Los certificados generados y firmados bajo la Infraestructura Nacional de Certificación Electrónica son los definidos para X.509v4, 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.

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

5.4.3 La versión contemplada para los certificados emitidos en la Infraestructura

Nacional de Certificación Electrónica es la versión 3 (Indicado por el entero 2).

5.4.4 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.

5.4.5 El algoritmo de firma es el algoritmo P-512 ecdsa-with-SHA512 para los Certificados Electrónicos de Entidad Final con longitud de cifrado de **512** bits y para los Certificados Electrónicos de AC, la longitud de cifrado es de **521** bits.

5.4.6 El campo Issuer del certificado contiene información que identifica inequívocamente al PSC, emisor del certificado electrónico. Dicha información es de tipo *Distinguished Name.*

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

5.4.8 El DN Serial Number (serialNumber) debe identificar al PSC a través de su Registro de Información Fiscal (R.I.F) (Anexo A).

5.4.9 La validez del certificado contiene la fecha exacta de emisión (notBefore) y de expiración del certificado (notAfter). Debe ser expresada en formato UTC (GMT 0) y coincidir con los límites establecidos por esta norma (vigencia en la Tabla N° 1).

5.4.10 El Titular (subject) del certificado contiene información que identifica inequívocamente al usuario del certificado electrónico, dicha información es de tipo Distinguished Name. El formato de dicho campo al igual que en Distinguished Name, debe garantizar que dichos atributos se pueden

diferenciar únicamente.

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

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

5.4.13 Los certificados deben poseer como mínimo las siguientes extensiones: Restricciones Básicas (basicConstraints), Uso de Clave (keyUsage), Identificador de Clave de la Autoridad Certificadora Emisora (issuerUniqueIdentifier), Puntos de Distribución de la LCR (cRLDistributionPoints), Acceso a la Información de Autoridad (authorityInfoAccess, AIA) y Políticas de Certificado (certificatePolicies).

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

5.4.15 La extensión Uso de Clave (KeyUsage) 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 (Anexo D).

Los valores Firma de Certificado y Firma de LCR, de Uso de Clave, están reservadas exclusivamente a los certificados de AC raíz, AC principal y AC subordinada.

En el valor de Uso de Clave se podrá usar “No Repudio” o “Compromiso o Vinculación con el Contenido“.

5.4.16 El Identificador de clave de Titular (subjectUniqueIdentifier) contiene el resultado de la Función Hash sobre la Clave Pública del Titular.

5.4.17 El Identificador de Clave de Autoridad Certificadora Emisora (issuerUniqueIdentifier) contiene el resultado de la Función Hash sobre la Clave Pública de la Autoridad de Certificación, nombre y serial de la misma.

5.4.18 El Uso Extendido de la Clave (extendedKeyUsage) puede ser de carácter crítico o no crítico y complementan la funcionalidad de un certificado. El PSC podrá incorporar tantos extendedKeyUsage como sean necesarios de acuerdo a la Política de Certificación (Anexo E).

5.4.19 Nombre Alternativo del Titular (issuerAltName) es una extensión de carácter no crítico, que debe contener uno o más nombres alternativos en formato de Nombres Generales (General Name – GN) (Anexo B).

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

5.4.21 En los Puntos de Distribución de las LCR (cRLDistributionPoints) se deben colocar al menos un punto para poder validar el estatus del certificado.

5.4.22 El Acceso a la Información de la Autoridad (authorityInfoAccess - AIA) está destinada a contener el método y URL donde se puede consultar el estatus del certificado. Éstos pueden ser servicios como LDAP, OCSP y otras soportadas por el estándar X.509.

5.4.23 La Política de Certificado (certificatePolicies) debe contener información que identifique las políticas bajo las cuales fue emitido el certificado y dónde se puede obtener dicha documentación. Si el PSC contiene más de una política u otra

documentación, la ubicación a la que hace referencia en esta extensión, debe proveer información que permita reconocer exactamente a cuál PC está asociado el certificado.

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

5.4.25 La Lista de Certificados Revocados es un instrumento de validación del estatus de un certificado electrónico definido en el RFC 5280. Ésta 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.

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

5.4.27 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.

5.4.28 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.

6. PARTE FINAL

6.1. Disposiciones transitorias

PRIMERA: 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), pasarán por un proceso de migración iniciando por la AC Raíz, a través del cual se generarán nuevos certificados electrónicos a las autoridades de certificación.

SEGUNDA: 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.

6.2. Disposiciones finales

PRIMERA: A partir de la fecha de publicación de esta norma en Gaceta Oficial de la República Bolivariana de Venezuela, se deberá iniciar por parte de los Proveedores de Servicios de Certificación acreditados, un proceso de actualización de sus políticas de certificación y las plantillas de los certificados electrónicos que no cumplan con lo aquí previsto.

SEGUNDA: Los PSC tendrán un período de 6 meses, contados a partir de la fecha de publicación de la presente norma, para dar cumplimiento al proceso de actualización antes mencionado. Durante ese lapso el PSC deberá consignar ante SUSCERTE informes trimestrales donde se evidencie el alcance y avance de esta actualización.

TERCERA: Al finalizar el proceso de actualización por parte del PSC, SUSCERTE deberá realizar una auditoría conforme a lo establecido en la Norma N° 59.

7. ANEXOS

Los anexos constituyen parte integral de la norma y deben ser de cumplimiento obligatorio

por los PSC.

7.1 Anexo A: Uso del *DN Serial Number*

Se debe utilizar para identificar únicamente al emisor, titular y/o propietario del certificado electrónico.

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

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 Pasaporte deberá incluir todos los dígitos de dicho documento.

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

El Registro Único de Información Fiscal (R.I.F.) deberá seguir el formato del ente emisor, ejemplo: V-00000000, G-000000000, J-000000000

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

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.

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

7.2 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

7.3 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

7.4 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 o 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, usando cifrado Diffie-Hellman.
Firma de certificado	keyCertSign(5)	Permite a las ACs firmar certificados electrónicos.
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.

7.5 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 Commercial 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

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

Perfil de Lista de Certificados Revocados		
Nombre(X.509)	**Tipo de dato [Constante] < Valor > (Observación)**	**Crítica (para extensiones)**
Datos de LCR		
Versión (versión)	Entero Hexadecimal [V2] < 0x1 > (X.509 v2 Formato CRL)	
Algoritmo de Firma (signature)	Algoritmo Autorizado (OID de los algoritmo permitido sha512WithECDSAEncryption)	
Datos de Emisor (issuer)		
Nombre Común (commonName)	UTF8 <Identificación de la AC Subordinada del Proveedor de Servicios de Certificación> **(Requerido)**	
Correo Electrónico (emailAddress)	UTF8 <Correo electrónico del ente que gestiona la AC> **(Opcional)**	
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> **(Opcional)**	
Organización (organization)	UTF8 [Sistema Nacional de Certificación Electrónica] **(Requerido)**	
Localidad(locality)	UTF8 <Dirección física del PSC> **(Opcional)**	
Estado(state)	UTF8 <Estado en el cual se ubica el PSC> **(Opcional)**	

País (country)	UTF8 [VE] (ISO 3166-1-alpha-2) **(Requerido)**	
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 (AuthorityKeyIdentifier)		
Clave de Autoridad (keyIdentifier)	KeyIdentifier <Identificador de la clave pública de la AC Raíz> **(Requerido)**	
Nombre distintivo (authorityCertIssuer)	GeneralName <Contiene la información de la AC Raíz con el formato DN > **(Requerido)**	
Serial (authorityCertSerialNumber)	CertificateSerialNumber <Contiene el número del certificado del emisor> **(Requerido)**	
Puntos de Distribución de las LCR (cRLDistributionPoints)		x
Punto de distribución LCR (distributionPoint)	<Dirección de descarga de la LCR por el PSC> (**Requerido)**	
Certificados Revocados		
Certificados revocados (Revoked Certificates)		
Serial del Certificado (Serial Number)	Entero Hexadecimal<Serial de certificado revocado > **(Requerido)**	
Fecha de revocación (Revocatión Date)	Fecha<fecha y hora en formato UTC> **(Requerido)**	
Razón de Revocación (CRL Reason Code)	Razón de Revocación < Ver Anexo G > **(Requerido)**	

Firma		
Algoritmo de Firma (signatureAlgorithm)	Algoritmo Autorizado (OID de los algoritmo permitido sha512WithECDSAEncryption)	
Firma(signature)	<Contenido de la Firma>	

7.6.1 El campo “issuer” de la LCR debe ser una copia fiel al campo “subject” del certificado de la CA emisora.

7.7 Anexo G: Razón de Revocación

Se utilizan para indicar la razón de revocación de un certificado en la LCR. X.509

Nombre	X.509
Sin Especificar	unspecified (0)
Compromiso de Clave	keyCompromise (1)
Compromiso de AC	cACompromise (2)
Cambio de Afiliación	affiliationChanged (3)
Sustitución	superseded (4)
Cese de operaciones	cessationOfOperation (5)
Retención de Certificado	certificateHold (6)
Borrado de LCR	removeFromCRL (8)
Retiro de privilegios	privilegeWithdrawn (9)
Compromiso de AA	aACompromise (10)

7.8 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. El atributo de género CONTENDRÁ, cuando esté presente, el valor del género del Titular. Para las mujeres se utilizará el valor "F" o "f", y para los hombres el valor "M" o "m". La forma en que se asocia el género al sujeto queda fuera del ámbito de esta especificación.
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”

7.9 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. El estándar ISO/IEC 19785-1

Nombre	X.509	Observación
		define una serie de valores OID (Object Identifiers) para el campo "typeOfBiometricData". Por defecto es una imagen de la firma autógrafa del titular (handwritten-signature).
Algoritmo de Hash	hashAlgorithm	Es la función hash utilizada para guiar 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.

7.10 Anexo J: Estructuras de Certificados

7.10.1 Estructura Certificado de la AC Raíz (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 > (Observación)**	**Crítica (para extensiones)**
Datos del Certificado		
Versión (versión)	Entero Hexadecimal [V4] < 0x2 >(Representa la versión 4 del X.509) (**Requerido)**	
Serial (serialNumber)	Entero Hexadecimal <Asignado por la AC> (No negativo) (**Requerido)**	

Algoritmo de Firma (signature)	Algoritmo Autorizado (OID de los algoritmo permitido sha512WithECDSAEncryption)	
Datos de Emisor (issuer)		
Nombre Común (commonName)	UTF8 [SUSCERTE] **(Requerido)**	
Organización (organization)	UTF8 [Sistema Nacional de Certificación Electrónica] **(Requerido)**	
País (country)	UTF8 [VE] (ISO 3166-1-alpha-2) **(Requerido)**	
Datos de Validez		
No Antes(notBefore)	Fecha (UTC)	
No Después(notAfter)	Fecha (UTC)	
Datos de Titular (subject)		
Nombre Común (commonName)	UTF8 [SUSCERTE] **(Requerido)**	
Organización (organization)	UTF8 [Sistema Nacional de Certificación Electrónica] **(Requerido)**	
País (country)	UTF8 [VE] (ISO 3166-1-alpha-2) **(Requerido)**	
Información de Clave Pública del Titular (subjectPublicKey)		
Algoritmo de Firma (signatureAlgorithm)	<Algoritmo Asignado> (ecdsaEncryption, dhpublicnumber,id-ecdsa, id-ecdsaPublicKey)	
Módulo(modulus)	Cadena de Octetos [512bit] **(Requerido)**	
ASN1 OID	secp521r1	
NIST CURVE	P-521	
* Para el caso de ECDSA se exigen los siguientes Módulos		
Extensiones		
Restricciones Básicas (basicConstraints) (Requerido)		**X**

Autoridad de Certificación(aC)	Booleano [true]	
Uso de la llave (keyUsage) (Requerido)		**X**
Firma de certificado	keyCertSign(5)	
Firma de LCR	cRLSign (6)	
Firma		
Algoritmo de Firma (signatureAlgorithm)	Algoritmo Autorizado (OID de los algoritmos permitidos mínimo sha512WithECDSAEncryption)	
Firma(signature)	<Contenido de la Firma>	

7.10.2 Estructura Certificado AC Principal

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

Certificado de la AC Principal		
Nombre(X.509)	**Tipo de dato [Constante] < Valor > (Observación)**	**Crítica (para extensiones)**
Datos del Certificado		
Versión (version)	Entero Hexadecimal [V4] < 0x2 >(Representa la versión 4 del X.509) **(Requerido)**	
Serial (serialNumber)	Entero Hexadecimal <Asignado por la AC> (No negativo) **(Requerido)**	
Algoritmo de Firma (signature)	Algoritmo Autorizado (OID de los algoritmo permitido sha512WithECDSAEncryption) **(Requerido)**	
Datos de Emisor (issuer)		
Nombre Común (commonName)	UTF8 [SUSCERTE] **(Requerido)**	
Organización (organization)	UTF8 [Sistema Nacional de Certificación Electrónica] **(Requerido)**	

País (country)	UTF8 [VE] (ISO 3166-1-alpha-2) **(Requerido)**	
Datos de Validez		
No Antes(notBefore)	Fecha (UTC)	
No Después(notAfter)	Fecha (UTC)	
Datos de Titular (subject)		
Nombre Común (commonName)	UTF8 <Identificación de la AC Subordinada del Proveedor de Servicios de Certificación> **(Requerido)**	
Correo Electrónico(emailAddress)	UTF8 <Correo electrónico del ente que gestiona la AC Subordinada> **(Opcional)**	
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> **(Opcional)**	
Organización (organization)	UTF8 [Sistema Nacional de Certificación Electrónica] **(Requerido)**	
Localidad(locality)	UTF8 <Dirección física del PSC> **(Opcional)**	
Estado(state)	UTF8 <Estado en el cual se ubica el PSC> **(Opcional)**	
País (country)	UTF8 [VE] (ISO 3166-1-alpha-2) **(Requerido)**	
Información de Clave Pública del Titular (subjectPublicKey)		
Algoritmo de Firma (signatureAlgorithm)	<Algoritmo Asignado> (ecdsaEncryption, dhpublicnumber,id-ecdsa, id-ecdsaPublicKey)	
Módulo(modulus) *	Cadena de Octetos [521 bit]	
* Para el caso de ECDSA se exigen los siguientes Módulo		
Extensiones		
Restricciones Básicas (basicConstraints) (Requerido)		**X**
Autoridad de	Booleano [true]	

Certificación(aC)		
Uso de la llave (keyUsage) (Requerido)		**X**
Firma de certificado	keyCertSign(5) **(Requerido)**	
Firma de LCR	cRLSign (6) **(Requerido)**	
Puntos de Distribución de las LCR (cRLDistributionPoints) (Requerido)		
Punto de distribución LCR (distributionPoint)	<Dirección de descarga de la LCR por el PSC>	
Políticas de Certificación (PolicyInformation)		
PolicyInformation (PC)		
policy identifier(s)	< OID Autorizado por SUSCERTE>	
cPSuir	<Dirección donde se puede descargar la PC >	
PolicyInformation (DPC)		
policyIdentifier	<OID Autorizado por SUSCERTE>	
cPSuri	<Dirección dónde se puede descargar la DPC>	
Firma		
Algoritmo de Firma (signatureAlgorithm)	Algoritmo Autorizado (OID de los algoritmos permitidos mínimo sha512WithECDSAEncryption)	
Firma(signature)	<Contenido de la Firma>	

7.10.3 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, firmar certificados y listas de certificados necesarias para su operación.

Certificado de la AC Subordinada del PSC

Nombre(X.509)	Tipo de dato [Constante] < Valor > (Observación)	Crítica (para extensiones)
Datos del Certificado		
Versión (versión)	Entero Hexadecimal [V4] < 0x2 >(Representa la versión 4 del X.509) **(Requerido)**	
Serial (serialNumber)	Entero Hexadecimal <Asignado por la AC> (No negativo) **(Requerido)**	
Algoritmo de Firma (signature)	Algoritmo Autorizado (OID de los algoritmos permitidos mínimo sha512WithECDSAEncryption) **(Requerido)**	
Datos de Emisor (issuer)		
Nombre Común (commonName)	UTF8 <Identificación de la AC Subordinada del Proveedor de Servicios de Certificación> **(Requerido)**	
Correo Electrónico(emailAddress)	UTF8 <Correo electrónico del ente que gestiona la AC Subordinada> **(Opcional)**	
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> **(Opcional)**	
Organización (organization)	UTF8 [Sistema Nacional de Certificación Electrónica] **(Requerido)**	
Localidad(locality)	UTF8 <Dirección física del PSC> **(Opcional)**	
Estado(state)	UTF8 <Estado en el cual se ubica el PSC> **(Opcional)**	
País (country)	UTF8 [VE] (ISO 3166-1-alpha-2) **(Requerido)**	
Datos de Validez		
No Antes(notBefore)	Fecha (UTC)	

No Después(notAfter)	Fecha (UTC)	
Datos de Titular (subject)		
Nombre Común (commonName)	UTF8 [Identificación de la AC Subordinada del Proveedor de Servicios de Certificación] **(Requerido)**	
Organización (organization)	UTF8 [Sistema Nacional de Certificación Electrónica] **(Requerido)**	
Departamento (organizationUnity)	UTF8 [Nombre o razón social tal cual aparezca en el documento constitutivo del ente que gestiona la AC Subordinada] **(opcional)**	
País (country)	UTF8 [VE] (ISO 3166-1-alpha-2) **(Requerido)**	
Correo Electrónico (emailAddress)	UTF8 <Correo electrónico del ente que gestiona la AC Subordinada> **(Opcional)**	
Teléfono (telephoneNumber)	UTF8 <Teléfono de contacto del Titular> **(Opcional)**	
Localidad(locality)	UTF8 <Dirección física del PSC> **(Opcional)**	
Estado(state)	UTF8 <Estado en el cual se ubica el PSC> **(Opcional)**	
Información de Clave Pública del Titular		
Algoritmo de clave pública (algorithm)	<Algoritmo Asignado> (ecdsaEncryption, dhpublicnumber,id-ecdsa, id-ecdsaPublicKey)	
Información de Clave Pública del Titular (subjectPublicKey)		
Módulo(modulus) *	Cadena de Octetos [521 bit]	
* Para el caso de ECDSA se exigen los siguientes Módulos (Requerido)		
Extensiones		
Restricciones Básicas (basicConstraints) (Requerido)		**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) **(Requerido)**	
Uso de la llave (keyUsage) (Requerido)		**x**

Firma de certificado	keyCertSign(5) **(Requerido)**	
Firma de LCR	cRLSign (6) **(Requerido)**	
Identificador de clave de Autoridad Certificadora (Authority Key Identifier) (Opcional)		
Clave de Autoridad(keyIdentifier)	KeyIdentifier <Identificador de la clave pública de la AC Raíz> **(Opcional)**	
Puntos de Distribución de las LCR (cRLDistributionPoints) (Requerido)		
Punto de distribución LCR (distributionPoint)	<Dirección de descarga de la LCR por el PSC>	
AIA (authorityInfoAccess) (Requerido)		
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) Aplica de acuerdo a las guías de ac-Browser)		
PolicyInformation (PC)		
Identificador de Política (policyIdentifier)	<OID Autorizado por SUSCERTE> **(Requerido)**	
Identificador de recurso uniforme (cPSuri)	<Dirección dónde se puede descargar la PC> **(Opcional)**	
PolicyInformation (DPC)		
policyIdentifier	<OID Autorizado por SUSCERTE>	
cPSuri	<Dirección dónde se puede descargar la DPC>	
Firma		
Algoritmo de Firma (signatureAlgorithm)	Algoritmo Autorizado (OID de los algoritmos	

	permitidos mínimo sha512WithECDSAEncryption)	
Firma(signature)	<Contenido de la Firma>	

7.10.4 Estructura del Certificado Persona Natural

Certificado cuyo signatario o titular es una persona natural, destinado 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 Persona Natural		
Nombre(X.509)	**Tipo de dato [Constante] <Valor> (Observación)**	**Crítica (para extensiones)**
Datos del Certificado		
Versión (versión)	Entero Hexadecimal [V4] < 0x2 >(Representa la versión 4 del X.509)	
Serial (serialNumber)	Entero Hexadecimal <Asignado por la AC> (No negativo)	
Algoritmo de Firma (signature)	Algoritmo Autorizado (OID de los algoritmo permitido sha512WithECDSAEncryption)	
Datos de Emisor (issuer)		
Nombre Común (commonName)	UTF8 <Identificación de la AC Subordinada del Proveedor de Servicios de Certificación> **(Requerido)**	
Correo Electrónico(emailAddress)	UTF8 <Correo electrónico del ente que gestiona la AC Subordinada> **(Opcional)**	
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> **(Opcional)**	
Organización (organization)	UTF8 [Sistema Nacional de Certificación	

	Electrónica] **(Requerido)**	
Localidad(locality)	UTF8 <Dirección física del Emisor> **(Opcional)**	
Estado(state)	UTF8 <Estado en el cual se ubica el Emisor> **(Opcional)**	
País (country)	UTF8 [VE] (ISO 3166-1-alpha-2) **(Requerido)**	
Datos de Validez		
No Antes(notBefore)	Fecha (UTC) **(Requerido)**	
No Después(notAfter)	Fecha (UTC) **(Requerido)**	
Datos de Titular (subject)		
Nombre Común (commonName)	UTF8 [Nombre1, Nombre2, Apellido1 y Apellido2] **(Requerido)**	
Correo Electrónico (emailAddress)	UTF8 <Dirección de correo electrónico de contacto del Titular> **(Opcional)**	
Teléfono (telephoneNumber)	UTF8 <Télefono de contacto del titular> **(Opcional)**	
Localidad(locality)	UTF8<Ciudad de residencia del Titular> **(Opcional)**	
Estado(state)	UTF8 <Estado de ubicación del Titular> **(Opcional)**	
País (country)	UTF8 [VE] (ISO 3166-1-alpha-2) **(Requerido)**	
SerialNumber (DN)	cédula de identidad (V o E), Registro Único de Información Fiscal (G o J) o Número de Pasaporte **(Requerido)**	
Información de Clave Pública del Titular (subjectPublicKey)		
Algoritmo de clave pública (algorithm)	<Algoritmo Asignado> (ecdsaEncryption, dhpublicnumber,id-ecdsa, id-ecdsaPublicKey)	
Módulo(modulus)*	Cadena de Octetos [521 bit] **(Requerido)**	
* Para el caso de ECDSA se exigen los siguientes Módulos (Requerido)		
Extensiones		
Restricciones Básicas (basicConstraints) (Requerido)		

Autoridad de Certificación(aC)	Booleano [false]	
Uso de la llave (keyUsage)(Opcional) (Requerido)		
Firma digital	digitalSignature(0)	
Compromiso de contenido(contentCommitment)	contentCommitment(1) - (No Repudio)	
Cifrado de Datos (dataEncipherment)	dataEncipherment(3)	
Identificador de clave de Autoridad Certificadora (Authority Key Identifier) (Opcional)		
Clave de Autoridad(keyIdentifier)	KeyIdentifier <Identificador de la clave pública de la AC Raíz>	
Usos Extendidos de la Clave (extKeyUsage) (Opcional)		
Autenticación del servidor	id-kp-clientAuth [RFC5280]	
Protección de correo electrónico	id-kp-emailProtection[RFC5280]	
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		

Puntos de Distribución de las LCR (cRLDistributionPoints) (Requerido)		
Punto de distribución LCR (distributionPoint)	<LCR del repositorio del PSC>	
AIA (authorityInfoAccess) (Requerido)		
Método de Acceso (accessMethod)	1.3.6.1.5.5.7.48.1 [OCSP]	
Dirección de Acceso (accessLocation)	<Dirección del servicio del OCSP del PSC>	
Políticas de Certificación (PolicyInformation) (Opcional)		
PolicyInformation (PC)		
policy identifier(s)	<OID Autorizado por SUSCERTE>	
cPSuir	<Dirección donde se puede descargar la PC>	
PolicyInformation (DPC) (Opcional)		
policyIdentifier	<OID Autorizado por SUSCERTE>	
cPSuri	<Dirección donde se puede descargar la DPC>	
Firma		
Algoritmo de Firma (signatureAlgorithm)	Algoritmo Autorizado (OID de los algoritmos sha512WithECDSAEncryption)	
Firma(signature)	<Contenido de la Firma>	

7.10.5 Estructura Certificado Persona Jurídica

Certificado cuyo signatario es una empresa u organización y el titular es una persona natural que representa legalmente a dicho ente destinado para firmar electrónicamente documentos y 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 Persona Jurídica		
Nombre(X.509)	**Tipo de dato [Constante] < Valor > (Observaciones)**	**Crítica (para extensiones)**
Datos del Certificado		
Versión (versión)	Entero Hexadecimal [V4] < 0x2 >(Representa la versión 4 del X.509) **(Requerido)**	
Serial (serialNumber)	Entero Hexadecimal <Asignado por la AC> (No negativo) **(Requerido)**	
Algoritmo de Firma (signature)	Algoritmo Autorizado (OID de los algoritmo permitido sha512WithECDSAEncryption)	
Datos de Emisor (issuer)		
Nombre Común (commonName)	UTF8 <Identificación de la AC Subordinada del Proveedor de Servicios de Certificación> **(Requerido)**	
Correo Electrónico(emailAddress)	UTF8 <Correo electrónico del ente que gestiona la AC Subordinada> **(Opcional)**	
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> **(Opcional)**	
Organización (organization)	UTF8 [Sistema Nacional de Certificación Electrónica] **(Requerido)**	
Localidad(locality)	UTF8 <Dirección física del Emisor> **(Opcional)**	
Estado(state)	UTF8 <Estado en el cual se ubica el Emisor> **(Opcional)**	
País (country)	UTF8 [VE] (ISO 3166-1-alpha-2) **(Requerido)**	
Datos de Validez		

No Antes(notBefore)	Fecha (UTC) **(Requerido)**	
No Después(notAfter)	Fecha (UTC) **(Requerido)**	
Datos de Titular (subject)		
Nombre Común (commonName)	UTF8 [Nombre1, Nombre2, Apellido1 y Apellido2] **(Requerido)**	
Serial (serialNumber)	UTF8 <Cédula, RIF o Pasaporte>(Ver Anexo A)**(Requerido)**	
Correo Electrónico (emailAddress)	UTF8 <Dirección de correo electrónico de contacto del Titular> **(Opcional)**	
Teléfono (telephoneNumber)	UTF8 <Télefono 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> **(Requerido)**	
Estado(state)	UTF8 <Estado de ubicación del Titular> **(Opcional)**	
País (country)	UTF8 [VE] (ISO 3166-1-alpha-2) (**Requerido)**	
Localidad(locality)	UTF8<Ciudad de residencia del titular> **(Opcional)**	
Información de Clave Pública del Titular (subjectPublicKey)		
Algoritmo de clave pública (algorithm)	<Algoritmo Asignado>(ecdsaEncryption, dhpublicnumber,id-ecdsa, id-ecdsaPublicKey)	
Módulo(modulus) *	Cadena de Octetos [521 bit]	
* Para el caso de ECDSA se exigen los siguientes campos **(Requerido)**		
Extensiones		
Restricciones Básicas (basicConstraints) (**Requerido)**		
Autoridad de Certificación(aC)	Booleano [false]	
Uso de la llave (keyUsage)		
Firma digital	digitalSignature(0)	

Compromiso de contenido(contentCommitment)	contentCommitment(1) - (No Repudio)	
Cifrado de Datos (dataEncipherment)	dataEncipherment(3)	
Identificador de clave de Autoridad Certificadora (Authority Key Identifier) (Opcional)		
Clave de Autoridad(keyIdentifier)	KeyIdentifier <Identificador de la clave pública de la AC Raíz>	
Usos Extendidos de la Clave (extKeyUsage) (Opcional)		
Autenticación del servidor	id-kp-clientAuth [RFC5280]	
Protección de correo electrónico	emailProtection 1.3.6.1.5.5.7.3.4	
Firma de Código	codeSigning 1.3.6.1.5.5.7.3.3	
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		
Puntos de Distribución de las LCR (cRLDistributionPoints) (Requerido)		

Punto de distribución LCR (distributionPoint)	<LCR del repositorio del PSC>	
AIA (authorityInfoAccess) (Requerido)		
Método de Acceso (accessMethod)	1.3.6.1.5.5.7.48.1 [OCSP]	
Dirección de Acceso (accessLocation)	<Dirección del servicio del OCSP del PSC>	
Políticas de Certificación (PolicyInformation) (Opcional)		
PolicyInformation (PC)		
policy identifier(s)	< OID Autorizado por SUSCERTE>	
cPSuir	<Dirección donde se puede descargar la PC >	
PolicyInformation (DPC)		
policyIdentifier	<OID Autorizado por SUSCERTE>	
cPSuri	<Dirección dónde se puede descargar la DPC>	
Firma		
Algoritmo de Firma (signatureAlgorithm)	Algoritmo Autorizado (OID de los algoritmos permitidos mínimo sha512WithECDSAEncryption)	
Firma(signature)	<Contenido de la Firma>	

7.10.6 Estructura Certificado Profesional Titulado

Certificado cuyo signatario o 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 Profesional Titulado

Nombre(X.509)	Tipo de dato [Constante] < Valor >	Crítica (para extensiones)
Datos del Certificado		
Versión (versión)	Entero Hexadecimal[V4] < 0x2 >(Representa la versión 4 del X.509) **(Requerido)**	
Serial (serialNumber)	Entero Hexadecimal <Asignado por la AC> (No negativo) **(Requerido)**	
Algoritmo de Firma (signature)	Algoritmo Autorizado (OID de los algoritmo permitido sha512WithECDSAEncryption)	
Datos de Emisor (issuer)		
Nombre Común (commonName)	UTF8 <Identificación de la AC Subordinada del Proveedor de Servicios de Certificación> **(Requerido)**	
Correo Electrónico(emailAddress)	UTF8 <Correo electrónico del ente que gestiona la AC Subordinada> **(Opcional)**	
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> **(Opcional)**	
Organización (organization)	UTF8 [Sistema Nacional de Certificación Electrónica] **(Requerido)**	
Localidad(locality)	UTF8 <Dirección física del Emisor> **(Opcional)**	
Estado(state)	UTF8 <Estado en el cual se ubica el Emisor> **(Opcional)**	
País (country)	UTF8 [VE] (ISO 3166-1-alpha-2) **(Requerido)**	

Datos de Validez		
No Antes(notBefore)	Fecha (UTC) **(Requerido)**	
No Después(notAfter)	Fecha (UTC) **(Requerido)**	
Datos de Titular (subject)		
Nombre Común (commonName)	UTF8 <Cadena compuesta por el nombre del Profesional y el número de Colegiado> **(Requerido)**	
Serial (serialNumber)	UTF8 <Cédula, RIF, Pasaporte> **(Requerido)**	
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> **(Requerido)**	
Correo Electrónico(emailAddress)	Dirección de correo electrónico de contacto del Titular **(Requerido)**	
Teléfono (telephoneNumber)	UTF8 <Número telefónico de contacto del Titular> **(Opcional)**	
Localidad (locality)	UTF8<Ciudad de ubicación del titular> **(Opcional)**	
Estado(state)	UTF8 <Estado de ubicación del Titular> **(Opcional)**	
País (country)	UTF8 [VE] (ISO 3166-1-alpha-2) **(Requerido)**	
Información de Clave Pública del Titular (subjectPublicKey)		
Algoritmo de clave pública (algorithm)	<Algoritmo Asignado>(ecdsaEncryption, dhpublicnumber,id-ecdsa, id-ecdsaPublicKey)	
Módulo(modulus)	Cadena de Octetos [521 bit] **(Requerido)**	
* Para el caso de ECDSA se exigen los siguientes Módulos		
Extensiones		

Restricciones Básicas (basicConstraints) (Requerido)		
Autoridad de Certificación(aC)	Booleano [false]	
Uso de la llave (keyUsage)		
Firma digital	digitalSignature(0)	
Compromiso de contenido(contentCommitment)	contentCommitment(1) - (No Repudio)	
Cifrado de Datos (dataEncipherment)	dataEncipherment(3)	
Identificador de clave de Autoridad Certificadora (Authority Key Identifier) (Opcional)		
Clave de Autoridad(keyIdentifier)	KeyIdentifier <Identificador de la clave pública de la AC Raíz>	
Usos Extendidos de la Clave (extKeyUsage) (Opcional)		
Autenticación del servidor	id-kp-clientAuth [RFC5280]	
Protección de correo electrónico	id-kp-emailProtection[RFC5280]	
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		
Puntos de Distribución de las LCR (cRLDistributionPoints) (Requerido)		
Punto de distribución LCR (distributionPoint)	<LCR del repositorio del PSC>	
AIA (authorityInfoAccess) (**Requerido)**		
Método de Acceso (accessMethod)	1.3.6.1.5.5.7.48.1 [OCSP]	
Dirección de Acceso (accessLocation)	<Dirección del servicio del OCSP del PSC>	
Políticas de Certificación (PolicyInformation) (Opcional)		
PolicyInformation (PC)		
policy identifier(s)	< OID Autorizado por SUSCERTE>	
cPSuir	<Dirección donde se puede descargar la PC>	
PolicyInformation (DPC)		
policyIdentifier	<OID Autorizado por SUSCERTE>	
cPSuri	<Dirección donde se puede descargar la DPC>	
Firma		
Algoritmo de Firma (signatureAlgorithm)	Algoritmo Autorizado (OID de los algoritmos permitidos mínimo sha512WithECDSAEncryption)	
Firma(signature)	<Contenido de la Firma>	

7.10.7 Estructura Certificado Empleado de Institución Pública

Certificado cuyo titular es una organización o ente del Estado y el signatario es una persona natural que desempeña actividades bajo relación laboral para dicha institución pública. El 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 Empleado de Institución Pública		
Nombre(X.509)	**Tipo de dato [Constante] < Valor >**	**Crítica (para extensiones)**
Datos del Certificado		
Versión (versión)	Entero Hexadecimal [V4] < 0x2 >(Representa la versión 4 del X.509) **(Requerido)**	
Serial (serialNumber)	Entero Hexadecimal <Asignado por la AC> (No negativo) **(Requerido)**	
Algoritmo de Firma (signature)	Algoritmo Autorizado (OID de los algoritmo permitido sha512WithECDSAEncryption)	
Datos de Emisor (issuer)		
Nombre Común (commonName)	UTF8 <Identificación de la AC Subordinada del Proveedor de Servicios de Certificación> **(Requerido)**	
Correo Electrónico(emailAddress)	UTF8 <Correo electrónico del ente que gestiona la AC Subordinada> **(Opcional)**	
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> **(Opcional)**	
Organización (organization)	UTF8 [Sistema Nacional de Certificación Electrónica] **(Requerido)**	
Localidad(locality)	UTF8 <Dirección física del Emisor>	

	(Opcional)	
Estado(state)	UTF8 <Estado en el cual se ubica el Emisor> **(Opcional)**	
País (country)	UTF8 [VE] (ISO 3166-1-alpha-2) **(Requerido)**	
Datos de Validez		
No Antes(notBefore)	Fecha (UTC) **(Requerido)**	
No Después(notAfter)	Fecha (UTC) **(Requerido)**	
Datos de Titular (subject)		
Nombre Común (commonName)	UTF8 [Nombre1, Nombre2, Apellido1 y Apellido2] **(Requerido)**	
Título(title)	UTF8<Título y/o cargo o funciones del titular del certificado> **(Requerido)**	
Correo Electrónico(emailAddress)	UTF8<Dirección de correo electrónico de contacto del Titular> **(Opcional)**	
Organización (organization)	UTF8<Nombre completo de la persona jurídica tal cual aparece en el documento constitutivo de la organización> **(Requerido)**	
Identificador de documento o Nombramiento (documentIdentifier)	UTF8 <Especificar documento que lo acredita como empleado> **(Requerido)**	
Teléfono (telephoneNumber)	UTF8 <Teléfono de contacto del Titular> **(Opcional)**	
Departamento (organizationUnity)	UTF8<Nombre del departamento, dirección o unidad de trabajo al cuál pertenece el titular> **(Opcional)**	
Localidad(locality)	UTF8 <Ciudad de ubicación del Titular> **(Opcional)**	
Estado(state)	UTF8 <Estado en el cual se ubica el	

	Titular> **(Opcional)**	
País (country)	UTF8 [VE] (ISO 3166-1-alpha-2) **(Requerido)**	
SerialNumber (DN)	cédula de identidad (V o E), Registro Único de Información Fiscal (G o J) o Número de Pasaporte **(Requerido)**	
Información de Clave Pública del Titular (subjectPublicKey)		
Algoritmo de clave pública (algorithm)	<Algoritmo Asignado>(ecdsaEncryption, dhpublicnumber,id-ecdsa, id-ecdsaPublicKey)	
Módulo(modulus)	Cadena de Octetos [521 bit] **(Requerido)**	
* Para el caso de ECDSA se exigen los siguientes Módulos		
Extensiones		
Restricciones Básicas (basicConstraints) (Requerido)		
Autoridad de Certificación(aC)	Booleano [false]	
Uso de la llave (keyUsage)		
Firma digital	digitalSignature(0)	
Compromiso de contenido(contentCommitment)	contentCommitment(1) - (No Repudio)	
Cifrado de Datos (dataEncipherment)	dataEncipherment(3)	
Identificador de clave de Autoridad Certificadora (Authority Key Identifier) (Opcional)		
Clave de Autoridad(keyIdentifier)	KeyIdentifier <Identificador de la clave pública de la AC Raíz>	
Usos Extendidos de la Clave (extKeyUsage) (Opcional)		
Autenticación del	id-kp-clientAuth [RFC5280]	

servidor		
Protección de correo electrónico	id-kp-emailProtection[RFC5280]	
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		
Puntos de Distribución de las LCR (cRLDistributionPoints) (Requerido)		
Punto de distribución LCR (distributionPoint)	<LCR del repositorio del PSC>	
AIA (authorityInfoAccess) (**Requerido)**		
Método de Acceso (accessMethod)	1.3.6.1.5.5.7.48.1 [OCSP]	
Dirección de Acceso (accessLocation)	<Dirección del servicio del OCSP del PSC>	
Políticas de Certificación (PolicyInformation) (Opcional)		
PolicyInformation (PC)		
policy identifier(s)	< OID Autorizado por SUSCERTE>	
cPSuir	<Dirección donde se puede descargar la PC >	

PolicyInformation (DPC)		
policyIdentifier	<OID Autorizado por SUSCERTE>	
cPSuri	<Dirección dónde se puede descargar la DPC>	
Firma		
Algoritmo de Firma (signatureAlgorithm)	Algoritmo Autorizado (OID de los algoritmos permitidos mínimo sha512WithECDSAEncryption)	
Firma(signature)	<Contenido de la Firma>	

7.10.8 Estructura Certificado de Empleado de Empresa Privada

Certificado cuyo titular es una empresa u organización y el signatario es una persona natural que está bajo relación laboral con dicho ente. Este certificado se destina para firmar electrónicamente documentos y 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 del Certificado		
Versión (versión)	Entero Hexadecimal [V4] < 0x2 >(Representa la versión 4 del X.509) **(Requerido)**	
Serial (serialNumber)	Entero Hexadecimal <Asignado por la AC> (No negativo) **(Requerido)**	
Algoritmo de Firma (signature)	Algoritmo Autorizado (OID de los algoritmo permitido sha512WithECDSAEncryption)	
Datos de Emisor (issuer)		
Nombre Común (commonName)	UTF8 [identificación de la AC principal O Subordinada] **(Requerido)**	

Organización (organization)	UTF8 [Sistema Nacional de Certificación Electrónica] **(Requerido)**	
Correo Electrónico(emailAddress)	UTF8 <Dirección de correo electrónico de contacto del Emisor> **(Opcional)**	
Teléfono (telephoneNumber)	UTF8 <Teléfono de contacto del Emisor> **(Opcional)**	
Departamento (organizationUnity)	UTF8 <Nombre o razón social tal cual aparezca en el documento constitutivo del ente que gestiona la AC Subordinada> **(Opcional)**	
Localidad(locality)	UTF8 <Ciudad de ubicación del Emisor> **(Opcional)**	
Estado(state)	UTF8 <Estado en el cual se ubica el Emisor> **(Opcional)**	
País (country)	UTF8 [VE] (ISO 3166-1-alpha-2) **(Requerido)**	
Datos de Validez		
No Antes(notBefore)	Fecha (UTC) **(Requerido)**	
No Después(notAfter)	Fecha (UTC) **(Requerido)**	
Datos de Titular (subject)		
Nombre Común (commonName)	UTF8 [Nombre1, Nombre2, Apellido1 y Apellido2] **(Requerido)**	
Organización (organization)	UTF8 [Nombre completo de la persona jurídica tal cual aparece en el documento constitutivo de la empresa] **(Requerido)**	
Título(title)	UTF8 <Título y/o cargo del empleado>**(Opcional)**	
Correo Electrónico (emailAddress)	UTF8 <Dirección de correo electrónico de contacto del Titular> **(Opcional)**	
Teléfono	UTF8 <Télefono de contacto del titular>	

(telephoneNumber)	**(Opcional)**	
Departamento (organizationUnity)	UTF8<Nombre del departamento, dirección o unidad de trabajo al cuál pertenece el titular> **(Opcional)**	
País (country)	UTF8 [VE] (ISO 3166-1-alpha-2) **(Requerido)**	
SerialNumber (DN)	cédula de identidad (V o E), Registro Único de Información Fiscal (G o J) o Número de Pasaporte **(Requerido)**	
Información de Clave Pública del Titular (subjectPublicKey)		
Algoritmo de clave pública (algorithm)	<AlgoritmoAsignado>(ecdsaEncryption, dhpublicnumber,id-ecdsa, id-ecdsaPublicKey)	
Módulo(modulus)	Cadena de Octetos [521 bit] **(Requerido)**	
* Para el caso de ECDSA se exigen en los siguientes Módulos		
Extensiones		
Restricciones Básicas (basicConstraints) (Requerido)		
Autoridad de Certificación(aC)	Booleano [false]	
Uso de la llave (keyUsage) (Requerido)		
Firma digital	digitalSignature(0)	
Compromiso de contenido(contentCommitment)	contentCommitment(1) - (No Repudio)	
Cifrado de Datos (dataEncipherment)	dataEncipherment(3)	
Identificador de clave de Autoridad Certificadora (Authority Key Identifier)		
Clave de Autoridad(keyIdentifi	KeyIdentifier <Identificador de la clave pública de la AC Raíz>	

er)		
Usos Extendidos de la Clave (extKeyUsage) Opcional		
Autenticación del servidor	id-kp-clientAuth [RFC5280]	
Protección de correo electrónico	id-kp-emailProtection[RFC5280]	
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		
Puntos de Distribución de las LCR (cRLDistributionPoints) (Requerido)		
Punto de distribución LCR (distributionPoint)	<LCR del repositorio del PSC>	
AIA (authorityInfoAccess) (Requerido)		
Método de Acceso (accessMethod)	1.3.6.1.5.5.7.48.1 [OCSP]	
Dirección de Acceso (accessLocation)	<Dirección del servicio del OCSP del PSC>	
Políticas de Certificación (PolicyInformation) (Opcional)		
PolicyInformation (PC)		

policy identifier(s)	< OID Autorizado por SUSCERTE>	
cPSuir	<Dirección donde se puede descargar la PC >	
PolicyInformation (DPC)		
policyIdentifier	<OID Autorizado por SUSCERTE>	
cPSuri	<Dirección dónde se puede descargar la DPC>	
Firma		
Algoritmo de Firma (signatureAlgorithm)	Algoritmo Autorizado (OID de los algoritmo permitido sha512WithECDSAEncryption)	
Firma(signature)	<Contenido de la Firma>	

7.10.9 Estructura de Certificado para la Cédula Electrónica

Certificado cuyo signatario o titular es una persona natural, destinado para su identificación y sólo podrá ser emitido por las autoridades de certificación del ente con competencia en identificación (SAIME). Posee atributos especiales para describir detalles de titular.

Certificado para la Cédula Electrónica		
Nombre(X.509)	**Tipo de dato [Constante] < Valor >**	**Crítica (para extensiones)**
Datos del Certificado		
Versión (versión)	Entero Hexadecimal [V4] < 0x2 >(Representa la versión 4 del X.509) **(Requerido)**	
Serial (serialNumber)	Entero Hexadecimal <Asignado por la AC> (No negativo) **(Requerido)**	
Algoritmo de Firma (signature)	Algoritmo Autorizado (OID de los algoritmo permitido sha512WithECDSAEncryption)	
Datos de Emisor (issuer)		

Nombre Común (commonName)	UTF8 <Identificación de la AC Subordinada del Proveedor de Servicios de Certificación> **(Requerido)**	
Correo Electrónico(emailAddress)	UTF8 <Correo electrónico del ente que gestiona la AC Subordinada> **(Opcional)**	
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> **(Opcional)**	
Organización (organization)	UTF8 [Sistema Nacional de Certificación Electrónica] **(Requerido)**	
Localidad(locality)	UTF8 <Dirección física del Emisor> **(Opcional)**	
Estado(state)	UTF8 <Estado en el cual se ubica el Emisor> **(Opcional)**	
País (country)	UTF8 [VE] (ISO 3166-1-alpha-2) **(Requerido)**	
Datos de Validez		
No Antes (notBefore)	Fecha (UTC) **(Requerido)**	
No Después (notAfter)	Fecha (UTC) **(Requerido)**	
Datos de Titular (subject)		
Nombre Común (commonName)	UTF8 [Nombre1, Nombre2, Apellido1 y Apellido2] **(Requerido)**	
SerialNumber (DN)	cédula de identidad (V o E), Registro Único de Información Fiscal (G o J) o Número de Pasaporte **(Requerido)**	
Correo Electrónico	UTF8 <Dirección de correo electrónico de	

(emailAddress)	contacto del Titular> **(Opcional)**	
Teléfono (telephoneNumber)	UTF8 <Télefono de contacto del titular> **(Opcional)**	
Calle (streetAddress)	UTF8 <Calle de residencia del Titular>**(Opcional)**	
Localidad(locality)	UTF8<Ciudad de residencia del Titular> **(Opcional)**	
Estado(state)	UTF8 <Estado de ubicación del Titular> **(Opcional)**	
País(country)	UTF8 [VE] (ISO 3166-1-alpha-2) **(Requerido)**	
Información de Clave Pública del Titular (subjectPublicKeyInfo)		
Algoritmo de clave pública (algorithm)	<Algoritmo Asignado>(ecdsaEncryption, dhpublicnumber,id-ecdsa, id-ecdsaPublicKey)	
Módulo(modulus)	Cadena de Octetos [521 bit] **(Requerido)**	
Atributos Adicionales del Titular (subjectDirectoryAttributes)		
Fecha de Nacimiento (dateOfBirth)	UTF8 <Fecha de Nacimiento del Titular> **(Obligatorio)**	
Lugar de Nacimiento (placeOfBirth)	UTF8 <Lugar de Nacimiento del Titular> **(Obligatorio)**	
Género (gender)	UTF8 male (masculino) o female (femenino) **(Obligatorio)**	
País de Ciudadanía (countryOfCitizenship)	UTF8 [VE] (ISO 3166-1-alpha-2) **(Obligatorio)**	
País de Residencia (countryOfResidence)	UTF8 [VE] (ISO 3166-1-alpha-2) **(Obligatorio)**	
Información Biométrica (biometricInfo) (Opcional)		
Tipos de datos	<Tipo de información biométrica que hace	

biométricos) (typeOfBiometricData)	referencia esta extensión>	
hashAlgorithm	<Es la función hash utilizada>	
Hash de datos biométricos (biometricDataHash)	Es el resultado de la función hash de la información biométrica.	
(sourceDataUri)	<Contiene la ubicación de dónde se almacena la información biométrica>	
Extensiones		
Restricciones Básicas (basicConstraints)		
Autoridad de Certificación(aC)	Booleano [false]	
Uso de la llave (keyUsage) (Requerido)		
Firma digital	digitalSignature(0)	
Compromiso de contenido(contentCommitment)	contentCommitment(1) - (No Repudio)	
Cifrado de Datos (dataEncipherment)	dataEncipherment(3)	
Identificador de clave de Autoridad Certificadora (Authority Key Identifier) (Opcional)		
Clave de Autoridad(keyIdentifier)	KeyIdentifier <Identificador de la clave pública de la AC Raíz>	
Usos Extendidos de la Clave (extKeyUsage) Opcional		
Autenticación del servidor	id-kp-clientAuth [RFC5280]	
Protección de correo electrónico	id-kp-emailProtection[RFC5280]	

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		
Puntos de Distribución de las LCR (cRLDistributionPoints) (Requerido)		
Punto de distribución LCR (distributionPoint)	<Dirección de descarga de la LCR del repositorio del PSC>	
AIA (authorityInfoAccess) (Requerido)		
Método de Acceso (accessMethod)	1.3.6.1.5.5.7.48.1 [OCSP]	
Dirección de Acceso (accessLocation)	<Dirección del servicio del OCSP del PSC>	
Políticas de Certificación (PolicyInformation) (Opcional)		
PolicyInformation (PC)		
policy identifier(s)	< OID Autorizado por SUSCERTE>	
cPSuir	<Dirección donde se puede descargar la PC >	
PolicyInformation (DPC)		
policyIdentifier	<OID Autorizado por SUSCERTE>	
cPSuri	<Dirección dónde se puede descargar la	

	DPC>	
Firma		
Algoritmo de Firma (signatureAlgorithm)	Algoritmo Autorizado (OID de los algoritmo permitido sha512WithECDSAEncryption)	
Firma(signature)	<Contenido de la Firma>	

7.10.10 Estructura Certificado de Servidor

Certificado cuyo signatario es una persona jurídica o natural, cuyo principal objetivo es identificar a un servicio web y proporcionarle seguridad a la comunicación. Entre las atribuciones 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, también 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 > (Observaciones)**	**Crítica (para extensiones)**
Datos del Certificado		
Versión (versión)	Entero Hexadecimal [V4] < 0x2 >(Representa la versión 4 del X.509)	
Serial (serialNumber)	Entero Hexadecimal <Asignado por la AC> (No negativo)	
Algoritmo de Firma (signature)	Algoritmo Autorizado (OID de los algoritmo permitido sha512WithECDSAEncryption)	
Datos de Emisor (issuer)		
Nombre Común (commonName)	UTF8 <Identificación de la AC Subordinada del Proveedor de Servicios	

	de Certificación> **(Requerido)**	
Correo Electrónico(emailAddress)	UTF8 <Correo electrónico del ente que gestiona la AC Subordinada> **(Opcional)**	
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> **(Opcional)**	
Organización (organization)	UTF8 [Sistema Nacional de Certificación Electrónica] **(Requerido)**	
Localidad(locality)	UTF8 <Dirección física del Emisor> **(Opcional)**	
Estado(state)	UTF8 <Estado en el cual se ubica el Emisor> **(Opcional)**	
País (country)	UTF8 [VE] (ISO 3166-1-alpha-2) **(Requerido)**	
Datos de Validez		
No Antes(notBefore)	Fecha (UTC) **(Requerido)**	
No Después(notAfter)	Fecha (UTC) **(Requerido)**	
Datos de Titular (subject)		
Nombre Común (commonName)	UTF8 [Identificación del servidor, dominio o aplicación] **(Requerido)**	
Serial (serialNumber)	UTF8 <RIF de la organización o empresa suscriptora del certificado> **(Requerido)**	
Correo Electrónico(emailAddress)	UTF8 <Correo electrónico de la Organización suscriptora>**(Requerido)**	
Teléfono (telephoneNumber)	UTF8 <Número telefónico del departamento que se encarga de la	

	administración y/o seguridad del servidor> **(Opcional)**	
Organización (organization)	UTF8<Nombre completo de la persona jurídica tal cual aparece en el documento constitutivo de la empresa suscriptora> **(Requerido)**	
Departamento (organizationUnity)	UTF8<Nombre del departamento, dirección o unidad de trabajo al cuál pertenece el titular> **(Opcional)**	
País (country)	UTF8 [VE] (ISO 3166-1-alpha-2) **(Requerido)**	
Categoría de Negocio (businessCategory)*	UTF8<"Private Organization" || " Government Entity" || " Business Entity" || "Non-Commercial Entity">(Sólo una de las siguientes opciones) **(Opcional)**	
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> **(Opcional)**	
Estado(state)	UTF8 <Estado donde se ubica organización suscriptora del certificado> **(Opcional)**	
* Necesarios para la Certificación EV		
Información de Clave Pública del Titular (subjectPublicKey)		

Algoritmo de clave pública (algorithm)	<Algoritmo Asignado>(ecdsaEncryption, dhpublicnumber,id-ecdsa, id-ecdsaPublicKey)	
Módulo(modulus)	Cadena de Octetos [521 bit] **(Requerido)**	
* Para el caso de ECDSA se exigen los siguientes Módulos		
Extensiones		
Restricciones Básicas (basicConstraints) (Requerido)		
Autoridad de Certificación(aC)	Booleano [false]	
Uso de la llave (keyUsage) (Requerido)		
Firma digital	digitalSignature(0)	
Compromiso de contenido(contentCommitment)	contentCommitment(1) - (No Repudio)	
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.		
Nombre Alternativo del Titular (subjectAltName) (Opcional)		
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)	
Usos Extendidos de la Clave (extKeyUsage) Opcional		

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		
Puntos de Distribución de las LCR (cRLDistributionPoints) (Requerido)		
Punto de distribución LCR (distributionPoint)	<Dirección de descarga de la LCR del repositorio del PSC>	
AIA (authorityInfoAccess) (Requerido)		
Método de Acceso (accessMethod)	1.3.6.1.5.5.7.48.1 [OCSP]	
Dirección de Acceso (accessLocation)	<Dirección del servicio del OCSP del PSC>	
Políticas de Certificación (PolicyInformation) (Opcional)		
PolicyInformation (PC)		
policy identifier(s)	< OID Autorizado por SUSCERTE>	
cPSuir	<Dirección donde se puede descargar la PC >	
PolicyInformation (DPC)		
policyIdentifier	<OID Autorizado por SUSCERTE>	
cPSuri	<Dirección dónde se puede descargar la DPC>	
Firma		
Algoritmo de Firma (signatureAlgorithm)	Algoritmo Autorizado (OID de los algoritmos permitidos mínimo sha512WithECDSAEncryption	

Firma(signature)	<Contenido de la Firma>	

7.10.11 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 del Certificado		
Versión (versión)	Entero Hexadecimal [V4] < 0x2 >(Representa la versión 4 del X.509) (**Requerido)**	
Serial (serialNumber)	Entero Hexadecimal <Asignado por la AC> (No negativo) (**Requerido)**	
Algoritmo de Firma (signature)	Algoritmo Autorizado (OID de los algoritmo permitido sha512WithECDSAEncryption)	
Datos de Emisor (issuer)		
Nombre Común (commonName)	UTF8 <Identificación de la AC Subordinada del Proveedor de Servicios de Certificación> **(Requerido)**	
Correo Electrónico(emailAddress)	UTF8 <Correo electrónico del ente que gestiona la AC Subordinada> **(Opcional)**	
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> **(Opcional)**	
Organización	UTF8 [Sistema Nacional de Certificación	

(organization)	Electrónica] **(Requerido)**	
Localidad(locality)	UTF8 <Dirección física del Emisor> **(Opcional)**	
Estado(state)	UTF8 <Estado en el cual se ubica el Emisor> **(Opcional)**	
País (country)	UTF8 [VE] (ISO 3166-1-alpha-2) **(Requerido)**	
Datos de Validez		
No Antes(notBefore)	Fecha (UTC) (**Requerido)**	
No Después(notAfter)	Fecha (UTC) (**Requerido)**	
Datos de Titular (subject)		
Nombre Común (commonName)	UTF8 [Nombre que identifica el servidor OCSP] (**Requerido)**	
Organización (organization)	UTF8 <Nombre o Razón social como aparece en documento constitutivo de la AC>	
Correo Electrónico (emailAddress)	UTF8 <Dirección de correo electrónico de la unidad responsabler> **(Opcional)**	
Localidad(locality)	UTF8 <Ciudad de ubicación del Titular> **(Opcional)**	
Estado(state)	UTF8 <Estado en el cual se ubica el Titular> **(Opcional)**	
País (country)	UTF8 [VE] (ISO 3166-1-alpha-2) (**Requerido)**	
Información de Clave Pública del Titular (subjectPublicKey)		
Algoritmo de clave pública (algorithm)	<Algoritmo Asignado>(ecdsaEncryption, dhpublicnumber,id-ecdsa, id-ecdsaPublicKey)	
Módulo(modulus)	Cadena de Octetos [521 bit] (**Requerido)**	
* Para el caso de ECDSA se exigen los siguientes Módulos		

Extensiones		
Restricciones Básicas (basicConstraints) (Requerido)		
Autoridad de Certificación(aC)	Booleano [false]	
Uso de la llave (keyUsage) (Requerido)		
Firma digital	digitalSignature(0)	
Compromiso de contenido(contentCommitment)	contentCommitment(1) - (No Repudio)	
Solo encriptar (encipherOnly)	keyEncipherment(2)	
Solo Descifrado (decipherOnly)	keyAgreement(4)	
Identificador de clave de Autoridad Certificadora (Authority Key Identifier) (Opcional)		
Clave de Autoridad(keyIdentifier)	KeyIdentifier <Identificador de la clave pública de la AC Raíz>	
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		
Puntos de Distribución de las LCR (cRLDistributionPoints) (Requerido)		
Punto de distribución LCR (distributionPoint)	<Dirección de descarga de la LCR del repositorio del PSC>	
AIA (authorityInfoAccess) (Requerido)		

Método de Acceso (accessMethod)	1.3.6.1.5.5.7.48.1 [OCSP]	
Dirección de Acceso (accessLocation)	<Dirección del servicio del OCSP del PSC>	
Políticas de Certificación (PolicyInformation) (Opcional)		
PolicyInformation (PC)		
policy identifier(s)	< OID Autorizado por SUSCERTE>	
cPSuir	<Dirección donde se puede descargar la PC >	
PolicyInformation (DPC)		
policyIdentifier	<OID Autorizado por SUSCERTE>	
cPSuri	<Dirección dónde se puede descargar la DPC>	
Firma		
Algoritmo de Firma (signatureAlgorithm)	Algoritmo Autorizado (OID de los algoritmo permitido sha512WithECDSAEncryption)	
Firma(signature)	<Contenido de la Firma>	

7.10.12 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 > (Observaciones)**	**Crítica (para extensiones)**
Datos del Certificado		

Versión (versión)	Entero Hexadecimal [V4] < 0x2 >(Representa la versión 4 del X.509) (**Requerido)**	
Serial (serialNumber)	Entero Hexadecimal <Asignado por la AC> (No negativo) (**Requerido)**	
Algoritmo de Firma (signature)	Algoritmo Autorizado (OID de los algoritmo permitido sha512WithECDSAEncryption)	
Datos de Emisor (issuer)		
Nombre Común (commonName)	UTF8 <Identificación de la AC Subordinada del Proveedor de Servicios de Certificación> **(Requerido)**	
Correo Electrónico(email Address)	UTF8 <Correo electrónico del ente que gestiona la AC Subordinada> **(Opcional)**	
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> **(Opcional)**	
Organización (organization)	UTF8 [Sistema Nacional de Certificación Electrónica] **(Requerido)**	
Localidad(locality)	UTF8 <Dirección física del Emisor> **(Opcional)**	
Estado(state)	UTF8 <Estado en el cual se ubica el Emisor> **(Opcional)**	
País (country)	UTF8 [VE] (ISO 3166-1-alpha-2) **(Requerido)**	
Datos de Validez		
No Antes (notBefore)	Fecha (UTC) (**Requerido)**	
No Después (notAfter)	Fecha (UTC) (**Requerido)**	
Datos de Titular (subject)		

Nombre Común (commonName)	UTF8 [Nombre1, Nombre2, Apellido1, Apellido2] **(Requerido)**	
Organización (organization)	UTF8 [Nombre completo de la persona jurídica tal cual aparece en el documento constitutivo de la empresa suscriptora] **(Requerido)**	
Correo Electrónico (emailAddress)	UTF8 <Dirección de correo electrónico de contacto del Titular> **(Opcional)**	
Teléfono (telephoneNumber)	UTF8 <Teléfono de contacto del titular> **(Opcional)**	
Departamento (organizationUnity)	UTF8<Nombre del departamento, dirección o unidad de trabajo al cual pertenece el titular> **(Opcional)**	
Localidad(locality)	UTF8<Ciudad donde se ubica el titular o suscriptor del certificado> **(Opcional)**	
Estado(state)	UTF8<Estado donde se ubica el titular o suscriptor del certificado> **(Opcional)**	
País (country)	UTF8 [VE] (ISO 3166-1-alpha-2) **(Requerido)**	
Serial(serialNumber)	UTF8 <IMEI del dispositivo movil> **(Requerido)**	
Información de Clave Pública del Titular (subjectPublicKey)		
Algoritmo de clave pública (algorithm)	<Algoritmo Asignado>(ecdsaEncryption, dhpublicnumber,id-ecdsa, id-ecdsaPublicKey)	
Módulo(modulus)	Cadena de Octetos [521 bit] (**Requerido)**	
* Para el caso de ECDSA se exigen los siguientes módulos		
Extensiones		
Restricciones Básicas (basicConstraints) (**Requerido)**		
Autoridad de Certificación(aC)	Booleano [false]	
Uso de la llave (keyUsage) (**Requerido)**		
Firma digital	digitalSignature(0)	

Compromiso de contenido(contentCommitment)	contentCommitment(1) - (No Repudio)	
Cifrado de claves	keyEncipherment(2)	
Acuerdo de claves	keyAgreement(4)	
** Se debe evaluar la aplicación de cada uno o combinación de estas Clave de Uso.		
Identificador de clave de Autoridad Certificadora (Authority Key Identifier) (Opcional)		
Clave de Autoridad(keyIdentifier)	KeyIdentifier <Identificador de la clave pública de la AC Raíz>	
Usos Extendidos de la Clave (extKeyUsage) (Opcional)		
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		
Puntos de Distribución de las LCR (cRLDistributionPoints) (Requerido)		
Punto de distribución LCR (distributionPoint)	<Dirección de descarga de la LCR del repositorio>	
AIA (authorityInfoAccess) (Requerido)		
Método de	1.3.6.1.5.5.7.48.1 [OCSP]	

Acceso (accessMethod)		
Dirección de Acceso (accessLocation)	<Dirección del servicio del OCSP del PSC> [URI:http://acraiz.suscerte.gob.ve/ocsp/]	
Políticas de Certificación (PolicyInformation) (Opcional)		
PolicyInformation (PC)		
policy identifier(s)	< OID Autorizado por SUSCERTE>	
cPSuir	<Dirección donde se puede descargar la PC >	
PolicyInformation (DPC)		
policyIdentifier	<OID Autorizado por SUSCERTE>	
cPSuri	<Dirección dónde se puede descargar la DPC>	
Firma		
Algoritmo de Firma (signatureAlgorithm)	Algoritmo Autorizado (OID de los algoritmo permitido sha512WithECDSAEncryption).	
Firma(signature)	<Contenido de la Firma>	

7.10.13 Estructura Certificado Electrónico de Banca Electrónica

Servicio que se utiliza para identificar al titular del certificado y verificar que el certificado sea válido, como también las transacciones bancarias electrónicas.

Los usuarios de banca electrónica emiten certificados con formato electrónico, emitidos de acuerdo con las disposiciones reglamentarias vigentes en el portal de la institución de banca por Internet. Transacciones electrónicas o no electrónicas realizadas por personas naturales o jurídicas, públicas o privadas, y los datos contenidos en cada transacción.

Banca Electrónica		
Nombre(X.509)	**Tipo de dato [Constante] < Valor >**	**Crítica (para extensiones)**
Datos del Certificado		
Versión (versión)	Entero Hexadecimal [V4] < 0x2 >(Representa la versión 4 del X.509)	
Serial (serialNumber)	Entero Hexadecimal <Asignado por la AC> (No negativo)	
Algoritmo de Firma (signature)	Algoritmo Autorizado (OID de los algoritmos permitidos mínimo sha512WithECDSAEncryption)	
Datos de Emisor (issuer)		
Nombre Común (commonName)	UTF8 <Identificación de la AC Subordinada del Proveedor de Servicios de Certificación> **(Requerido)**	
Correo Electrónico(emailAddress)	UTF8 <Correo electrónico del ente que gestiona la AC Subordinada> **(Opcional)**	
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> **(Opcional)**	
Organización (organization)	UTF8 [Sistema Nacional de Certificación Electrónica] **(Requerido)**	
Localidad(locality)	UTF8 <Dirección física del Emisor> **(Opcional)**	
Estado(state)	UTF8 <Estado en el cual se ubica el Emisor> **(Opcional)**	
País (country)	UTF8 [VE] (ISO 3166-1-alpha-2) **(Requerido)**	
Datos de Validez		
No Antes(notBefore)	Fecha (UTC) (**Requerido)**	
No	Fecha (UTC) (**Requerido)**	

Después(notAfter)		
Datos de Titular (subject)		
Nombre Común (commonName)	UTF8 [Nombre de la empresa o usuario a certificar] **(Requerido)**	
Organización (organization)	UTF8 [Nombre de entidad bancaria] **(Requerido)**	
Título (title)	Cargo del Titular **(Opcional)**	
País (country)	UTF8 [VE] (ISO 3166-1-alpha-2) (**Requerido)**	
Departamento (organizationUnity)	Nombre del representante de Empresa o usuario si es persona natural **(Opcional)**	
Correo Electrónico (emailAddress)	UTF8 <Dirección de correo electrónico de contacto del Titular> **(Opcional)**	
Localidad(locality)	Dirección fiscal de la Entidad Bancaria **(Requerido)**	
Estado(state)	UTF8 <Estado de ubicación del Titular> **(Opcional)**	
País(country)	UTF8 [VE] (ISO 3166-1-alpha-2) **(Requerido)**	
Información de Clave Pública del Titular (subjectPublicKey)		
Algoritmo de clave pública (algorithm)	<Algoritmo Asignado>(ecdsaEncryption, dhpublicnumber,id-ecdsa, id-ecdsaPublicKey)	
Módulo(modulus)	Cadena de Octetos [521 bit] (**Requerido)**	
* Para el caso de ECDSA se exigen los siguientes módulos		
Extensiones		
Restricciones Básicas (basicConstraints) (**Requerido)**		
Autoridad de Certificación(aC)	Booleano [false]	
Uso de la llave (keyUsage) (**Requerido)**		
Firma digital	digitalSignature(0)	
Compromiso de contenido(contentCommitment)	contentCommitment(1) - (No Repudio)	

Cifrado de Datos (dataEncipherment)	dataEncipherment(3)	
Identificador de clave de Autoridad Certificadora (Authority Key Identifier) (Opcional)		
Clave de Autoridad(keyIdentifier)	KeyIdentifier <Identificador de la clave pública de la AC Raíz>	
Usos Extendidos de la Clave (extKeyUsage) (Opcional)		
Autenticación del servidor	id-kp-clientAuth [RFC5280]	
Protección de correo electrónico	id-kp-emailProtection[RFC5280]	
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		
Puntos de Distribución de las LCR (cRLDistributionPoints) (Requerido)		
Punto de distribución LCR (distributionPoint)	<Dirección de descarga de la LCR del repositorio del PSC>	
AIA (authorityInfoAccess) (Requerido)		

Método de Acceso (accessMethod)	1.3.6.1.5.5.7.48.1 [OCSP]	
Dirección de Acceso (accessLocation)	<Dirección del servicio del OCSP del PSC>	
Políticas de Certificación (PolicyInformation) (Opcional)		
PolicyInformation (PC)		
policy identifier(s)	< OID Autorizado por SUSCERTE>	
cPSuir	<Dirección donde se puede descargar la PC >	
PolicyInformation (DPC)		
policyIdentifier	<OID Autorizado por SUSCERTE>	
cPSuri	<Dirección dónde se puede descargar la DPC>	
Firma		
Algoritmo de Firma (signatureAlgorithm)	Algoritmo Autorizado (OID de los algoritmo permitido sha512WithECDSAEncryption	
Firma(signature)	<Contenido de la Firma>	

7.10.14 Certificado de Firma Electrónica para Representante de Empresa Pública

Certificado cuyo titular es una empresa pública y el signatario es una persona natural que está bajo representación legal de una empresa pública. Este certificado se destina para firmar electrónicamente documentos y mensajes de datos, para expresar la voluntad de la empresa. Se pueden obtener diversas aplicaciones utilizando combinación de Claves de Usos y Claves de Usos Extendidos.

Representante de Empresa Pública		
Nombre(X.509)	**Tipo de dato [Constante] < Valor >**	**Crítica (para extensiones)**

Datos del Certificado		
Versión (versión)	Entero Hexadecimal [V4] < 0x2 >(Representa la versión 4 del X.509)	
Serial (serialNumber)	Entero Hexadecimal <Asignado por la AC> (No negativo)	
Algoritmo de Firma (signature)	Algoritmo Autorizado (OID de los algoritmo permitido sha512WithECDSAEncryption)	
Datos de Emisor (issuer)		
Nombre Común (commonName)	UTF8 <Identificación de la AC Subordinada del Proveedor de Servicios de Certificación> **(Requerido)**	
Correo Electrónico(emailAddress)	UTF8 <Correo electrónico del ente que gestiona la AC Subordinada> **(Opcional)**	
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> **(Opcional)**	
Organización (organization)	UTF8 [Sistema Nacional de Certificación Electrónica] **(Requerido)**	
Localidad(locality)	UTF8 <Dirección física del Emisor> **(Opcional)**	
Estado(state)	UTF8 <Estado en el cual se ubica el Emisor> **(Opcional)**	
País (country)	UTF8 [VE] (ISO 3166-1-alpha-2) **(Requerido)**	
Datos de Validez		
No Antes(notBefore)	Fecha (UTC) (**Requerido)**	
No Después(notAfter)	Fecha (UTC) (**Requerido)**	
Datos de Titular (subject)		
Nombre Común	UTF8 [Nombre1, Nombre2, Apellido1 y Apellido2]	

(commonName)	**(Requerido)**	
Organización (organization)	UTF8 [Nombre completo de la persona jurídica tal cual aparece en el documento constitutivo de la empresa] **(Requerido)**	
Título(title)	UTF8 <Título y/o cargo del empleado>**(Requerido)**	
Correo Electrónico (emailAddress)	UTF8 <Dirección de correo electrónico de contacto del Titular> **(Opcional)**	
Localidad(locality)	UTF8 <Ciudad de ubicación del Titular> **(Opcional)**	
Departamento (organizationUnity)	UTF8<Nombre del departamento, dirección o unidad de trabajo al cual pertenece el titular> **(Requerido)**	
País (country)	UTF8 [VE] (ISO 3166-1-alpha-2) **(Requerido)**	
Estado(state)	UTF8 <Estado en el cual se ubica el Titular> **(Opcional)**	
Información de Clave Pública del Titular (subjectPublicKey)		
Algoritmo de clave pública (algorithm)	<Algoritmo Asignado>(ecdsaEncryption, dhpublicnumber,id-ecdsa, id-ecdsaPublicKey)	
Módulo(modulus)	Cadena de Octetos [521 bit] (**Requerido)**	
* Para el caso de ECDSA se exigen los siguientes Módulos		
Extensiones		
Restricciones Básicas (basicConstraints) (**Requerido)**		
Autoridad de Certificación(aC)	Booleano [false]	
Uso de la llave (keyUsage) (**Requerido)**		
Firma digital	digitalSignature(0)	
Compromiso de contenido(contentCommitment)	contentCommitment(1) - (No Repudio)	
Cifrado de Datos (dataEncipherment)	dataEncipherment(3)	

Identificador de clave de Autoridad Certificadora (Authority Key Identifier) (Opcional)		
Clave de Autoridad(keyIdentifier)	KeyIdentifier <Identificador de la clave pública de la AC Raíz>	
Usos Extendidos de la Clave (extKeyUsage) (Opcional)		
Autenticación del servidor	id-kp-clientAuth [RFC5280]	
Protección de correo electrónico	id-kp-emailProtection[RFC5280]	
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		
Puntos de Distribución de las LCR (cRLDistributionPoints) (Requerido)		
Punto de distribución LCR (distributionPoint)	<Dirección de descarga de la LCR del repositorio del PSC>	
AIA (authorityInfoAccess) (Requerido)		
Método de Acceso (accessMethod)	1.3.6.1.5.5.7.48.1 [OCSP]	
Dirección de Acceso	<Dirección del servicio del OCSP del PSC>	

(accessLocation)		
Políticas de Certificación (PolicyInformation) (Opcional)		
PolicyInformation (PC)		
policy identifier(s)	< OID Autorizado por SUSCERTE>	
cPSuir	<Dirección donde se puede descargar la PC >	
PolicyInformation (DPC)		
policyIdentifier	<OID Autorizado por SUSCERTE>	
cPSuri	<Dirección dónde se puede descargar la DPC>	
Firma		
Algoritmo de Firma (signatureAlgorithm)	Algoritmo Autorizado (OID de los algoritmo permitido sha512WithECDSAEncryption	
Firma(signature)	<Contenido de la Firma>	

7.10.15 Certificado de Firma Electrónica para Representante de Empresa Privada

Certificado cuyo titular es una empresa privada y el signatario es una persona natural que está bajo representación legal de una empresa privada. Este certificado se destina para firmar electrónicamente documentos y mensajes de datos, para expresar la voluntad de la empresa. Se pueden obtener diversas aplicaciones utilizando combinación de Claves de Usos y Claves de Usos Extendidos.

Representante de Empresa Privada		
Nombre(X.509)	**Tipo de dato [Constante] < Valor >**	**Crítica (para extensiones)**
Datos del Certificado		
Versión (versión)	Entero Hexadecimal [V4] < 0x2 >(Representa la versión 4 del X.509)	
Serial (serialNumber)	Entero Hexadecimal <Asignado por la AC> (No negativo)	

Algoritmo de Firma (signature)	Algoritmo Autorizado (OID de los algoritmo permitido sha512WithECDSAEncryption)	
Datos de Emisor (issuer)		
Nombre Común (commonName)	UTF8 <Identificación de la AC Subordinada del Proveedor de Servicios de Certificación> **(Requerido)**	
Correo Electrónico(emailAddress)	UTF8 <Correo electrónico del ente que gestiona la AC Subordinada> **(Opcional)**	
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> **(Opcional)**	
Organización (organization)	UTF8 [Sistema Nacional de Certificación Electrónica] **(Requerido)**	
Localidad(locality)	UTF8 <Dirección física del Emisor> **(Opcional)**	
Estado(state)	UTF8 <Estado en el cual se ubica el Emisor> **(Opcional)**	
País (country)	UTF8 [VE] (ISO 3166-1-alpha-2) **(Requerido)**	
Datos de Validez		
No Antes(notBefore)	Fecha (UTC) (**Requerido)**	
No Después(notAfter)	Fecha (UTC) (**Requerido)**	
Datos de Titular (subject)		
Nombre Común (commonName)	UTF8 [Nombre1, Nombre2, Apellido1 y Apellido2] **(Requerido)**	
Organización (organization)	UTF8 [Nombre completo de la persona jurídica tal cual aparece en el documento constitutivo de la empresa] **(Requerido)**	
Título(title)	UTF8 <Título y/o cargo del empleado>**(Requerido)**	

Correo Electrónico (emailAddress)	UTF8 <Dirección de correo electrónico de contacto del Titular> **(Opcional)**	
Localidad(locality)	UTF8 <Ciudad de ubicación del Titular> **(Opcional)**	
Departamento (organizationUnity)	UTF8<Nombre del departamento, dirección o unidad de trabajo al cual pertenece el titular> **(Requerido)**	
País (country)	UTF8 [VE] (ISO 3166-1-alpha-2) **(Requerido)**	
Estado(state)	UTF8 <Estado en el cual se ubica el Titular> **(Opcional)**	
Información de Clave Pública del Titular (subjectPublicKey)		
Algoritmo de clave pública (algorithm)	<Algoritmo Asignado>(ecdsaEncryption, dhpublicnumber,id-ecdsa, id-ecdsaPublicKey)	
Módulo(modulus)	Cadena de Octetos [521 bit] (**Requerido)**	
* Para el caso de ECDSA se exigen los siguientes Módulos		
Extensiones		
Restricciones Básicas (basicConstraints) (Requerido)		
Autoridad de Certificación(aC)	Booleano [false]	
Uso de la llave (keyUsage) (Requerido)		
Firma digital	digitalSignature(0)	
Compromiso de contenido(contentCommitment)	contentCommitment(1) - (No Repudio)	
Cifrado de Datos (dataEncipherment)	dataEncipherment(3)	
Identificador de clave de Autoridad Certificadora (Authority Key Identifier) (Opcional)		

Clave de Autoridad(keyIdentifier)	KeyIdentifier <Identificador de la clave pública de la AC Raíz>	
Usos Extendidos de la Clave (extKeyUsage) (Opcional)		
Autenticación del servidor	id-kp-clientAuth [RFC5280]	
Protección de correo electrónico	id-kp-emailProtection[RFC5280]	
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		
Puntos de Distribución de las LCR (cRLDistributionPoints) (Requerido)		
Punto de distribución LCR (distributionPoint)	<Dirección de descarga de la LCR del repositorio del PSC>	
AIA (authorityInfoAccess) (Requerido)		
Método de Acceso (accessMethod)	1.3.6.1.5.5.7.48.1 [OCSP]	
Dirección de Acceso (accessLocation)	<Dirección del servicio del OCSP del PSC>	
Políticas de Certificación (PolicyInformation) (Opcional)		
PolicyInformation (PC)		

policy identifier(s)	< OID Autorizado por SUSCERTE>	
cPSuir	<Dirección donde se puede descargar la PC >	
PolicyInformation (DPC)		
policyIdentifier	<OID Autorizado por SUSCERTE>	
cPSuri	<Dirección dónde se puede descargar la DPC>	
Firma		
Algoritmo de Firma (signatureAlgorithm)	Algoritmo Autorizado (OID de los algoritmos permitidos sha512WithECDSAEncryption)	
Firma(signature)	<Contenido de la Firma>	

7.10.16 Estructura Certificado Electrónico para Control de Acceso Lógico

Tarjetas inteligentes que admiten todas las tecnologías de seguridad: autenticación, almacenamiento de archivos de contraseñas, certificados de infraestructura de clave pública, contraseñas de un solo uso, plantillas de imágenes biométricas y generación de pares de claves de acceso asimétrico. Las tarjetas inteligentes utilizadas junto con una o más tecnologías de autenticación proporcionan una autenticación mejorada para incrementar significativamente la seguridad del acceso lógico.

Control de Acceso Lógico		
Nombre(X.509)	**Tipo de dato [Constante] < Valor >**	**Crítica (para extensiones)**
Datos del Certificado		
Versión (versión)	Entero Hexadecimal [V4] < 0x2 >(Representa la versión 4 del X.509)	
Serial (serialNumber)	Entero Hexadecimal <Asignado por la AC> (No negativo)	
Algoritmo de Firma (signature)	Algoritmo Autorizado (OID de los algoritmos	

	permitidos sha512WithECDSAEncryption)	
Datos de Emisor (issuer)		
Nombre Común (commonName)	UTF8 <Identificación de la AC Subordinada del Proveedor de Servicios de Certificación> **(Requerido)**	
Correo Electrónico(emailAddress)	UTF8 <Correo electrónico del ente que gestiona la AC Subordinada> **(Opcional)**	
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> **(Opcional)**	
Organización (organization)	UTF8 [Sistema Nacional de Certificación Electrónica] **(Requerido)**	
Localidad(locality)	UTF8 <Dirección física del Emisor> **(Opcional)**	
Estado(state)	UTF8 <Estado en el cual se ubica el Emisor> **(Opcional)**	
País (country)	UTF8 [VE] (ISO 3166-1-alpha-2) **(Requerido)**	
Datos de Validez		
No Antes(notBefore)	Fecha (UTC) (**Requerido)**	
No Después(notAfter)	Fecha (UTC) (**Requerido)**	
Datos de Titular (subject)		
Nombre Común (commonName)	UTF8 [Nombre que identifica el servicio de la tarjeta inteligente] **(Requerido)**	
Organización (organization)	UTF8 [Nombre completo de la persona jurídica tal cual aparece en el documento constitutivo de la empresa suscriptora] **(Requerido)**	
Correo Electrónico (emailAddress)	UTF8 <Dirección de correo electrónico de contacto del Titular> **(Opcional)**	

Título (title)	Dirección IP / DNS **(Requerido)**	
Departamento (organizationUnity)	UTF8<Nombre del departamento, dirección o unidad de trabajo al cual pertenece el titular> **(Opcional)**	
Localidad(locality)	UTF8<Ciudad donde se ubica el titular o suscriptor del certificado> **(Opcional)**	
Estado(state)	UTF8<Estado donde se ubica el titular o suscriptor del certificado> **(Opcional)**	
País (country)	UTF8 [VE] (ISO 3166-1-alpha-2) **(Requerido)**	
Correo Electrónico(emailAddress)	Dirección de correo electrónico de contacto del Titular **(Opcional)**	
Información de Clave Pública del Titular (subjectPublicKey)		
Algoritmo de clave pública (algorithm)	<Algoritmo Asignado>(ecdsaEncryption, dhpublicnumber,id-ecdsa, id-ecdsaPublicKey)	
Módulo(modulus)	Cadena de Octetos [521 bit] **(Requerido)**	
* Para el caso de ECDSA se exigen los siguientes módulos		
Extensiones		
Restricciones Básicas (basicConstraints) (**Requerido)**		
Autoridad de Certificación(aC)	Booleano [false]	
Uso de la llave (keyUsage) (**Requerido)**		
Firma digital	digitalSignature(0)	
Compromiso de contenido(contentCommitment)	contentCommitment(1) - (No Repudio)	
Cifrado de Datos (dataEncipherment)	dataEncipherment(3)	
Identificador de clave de Autoridad Certificadora (Authority Key Identifier) (Opcional)		
Clave de	KeyIdentifier <Identificador de la clave pública de	

Autoridad(keyIdentifier)	la AC Raíz>	
Usos Extendidos de la Clave (extKeyUsage) (Opcional)		
Autenticación del servidor	id-kp-clientAuth [RFC5280]	
Protección de correo electrónico	id-kp-emailProtection[RFC5280]	
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		
Puntos de Distribución de las LCR (cRLDistributionPoints) (Requerido)		
Punto de distribución LCR (distributionPoint)	<Dirección de descarga de la LCR del repositorio del PSC>	
AIA (authorityInfoAccess) (Requerido)		
Método de Acceso (accessMethod)	1.3.6.1.5.5.7.48.1 [OCSP]	
Dirección de Acceso (accessLocation)	<Dirección del servicio del OCSP del PSC>	
Políticas de Certificación (PolicyInformation) (Opcional)		
PolicyInformation (PC)		

policy identifier(s)	< OID Autorizado por SUSCERTE>	
cPSuir	<Dirección donde se puede descargar la PC >	
PolicyInformation (DPC)		
policyIdentifier	<OID Autorizado por SUSCERTE>	
cPSuri	<Dirección dónde se puede descargar la DPC>	
Firma		
Algoritmo de Firma (signatureAlgorithm)	Algoritmo Autorizado (OID de los algoritmos permitidos sha512WithECDSAEncryption	
Firma(signature)	<Contenido de la Firma>	

7.10.17 Certificado Electrónico de Firma de Transacción

Los certificados de firma de transacciones garantizan la integridad y el no repudio de las transacciones electrónicas, realizadas por personas naturales o jurídicas, de los datos contenidos en cada transacción.

Firma de Transacción		
Nombre(X.509)	**Tipo de dato [Constante] < Valor >**	**Crítica (para extensiones)**
Datos del Certificado		
Versión (versión)	Entero Hexadecimal [V4] < 0x2 >(Representa la versión 4 del X.509)	
Serial (serialNumber)	Entero Hexadecimal <Asignado por la AC> (No negativo)	
Algoritmo de Firma (signature)	Algoritmo Autorizado (OID de los algoritmo permitido sha512WithECDSAEncryption)	

Datos de Emisor (issuer)		
Nombre Común (commonName)	UTF8 <Identificación de la AC Subordinada del Proveedor de Servicios de Certificación> **(Requerido)**	
Correo Electrónico(emailAddress)	UTF8 <Correo electrónico del ente que gestiona la AC Subordinada> **(Opcional)**	
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> **(Opcional)**	
Organización (organization)	UTF8 [Sistema Nacional de Certificación Electrónica] **(Requerido)**	
Localidad(locality)	UTF8 <Dirección física del Emisor> **(Opcional)**	
Estado(state)	UTF8 <Estado en el cual se ubica el Emisor> **(Opcional)**	
País (country)	UTF8 [VE] (ISO 3166-1-alpha-2) **(Requerido)**	
Datos de Validez		
No Antes(notBefore)	Fecha (UTC) **(Requerido)**	
No Después(notAfter)	Fecha (UTC) **(Requerido)**	
Datos de Titular (subject)		
Nombre Común (commonName)	Identificador del objeto **(Requerido)**	
Organización (organization)	UTF8 [Nombre completo de la organización tal cual aparece en el documento constitutivo de la empresa suscriptora] **(Requerido)**	
Correo Electrónico (emailAddress)	UTF8 <Dirección de correo electrónico de contacto del Titular> **(Opcional)**	
Título (Title)	Ubicación **(Opcional)**	

Departamento (organizationUnity)	UTF8<Nombre del departamento, dirección o unidad de trabajo al cual pertenece el titular> **(Opcional)**	
Localidad(locality)	UTF8<Ciudad donde se ubica el titular o suscriptor del certificado> **(Opcional)**	
Estado(state)	UTF8<Estado donde se ubica el titular o suscriptor del certificado>	
País (country)	UTF8 [VE] (ISO 3166-1-alpha-2) **(Requerido)**	
SerialNumber (DN)	Número de RIF **(Requerido)**	
Información de Clave Pública del Titular (subjectPublicKey)		
Algoritmo de clave pública (algorithm)	<Algoritmo Asignado>(ecdsaEncryption, dhpublicnumber,id-ecdsa, id-ecdsaPublicKey)	
Módulo(modulus)	Cadena de Octetos [521 bit] (**Requerido)**	
* Para el caso de ECDSA se exigen los siguientes módulos		
Extensiones		
Restricciones Básicas (basicConstraints) (Requerido)		
Autoridad de Certificación(aC)	Booleano [false]	
Uso de la llave (keyUsage) (Requerido)		
Firma digital	digitalSignature(0)	
Compromiso de contenido(contentCommitment)	contentCommitment(1) - (No Repudio)	
Cifrado de Datos (dataEncipherment)	dataEncipherment(3)	
Identificador de clave de Autoridad Certificadora (Authority Key Identifier) (Opcional)		
Clave de Autoridad(keyIdentifier)	KeyIdentifier <Identificador de la clave pública de la AC Raíz>	

Usos Extendidos de la Clave (extKeyUsage) (Opcional)		
Autenticación del servidor	id-kp-clientAuth [RFC5280]	
Protección de correo electrónico	id-kp-emailProtection[RFC5280]	
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		
Puntos de Distribución de las LCR (cRLDistributionPoints) (Requerido)		
Punto de distribución LCR (distributionPoint)	<Dirección de descarga de la LCR del repositorio del PSC>	
AIA (authorityInfoAccess) (Requerido)		
Método de Acceso (accessMethod)	1.3.6.1.5.5.7.48.1 [OCSP]	
Dirección de Acceso (accessLocation)	<Dirección del servicio del OCSP del PSC>	
Políticas de Certificación (PolicyInformation) (Opcional)		
PolicyInformation (PC)		
policy identifier(s)	< OID Autorizado por SUSCERTE>	
cPSuir	<Dirección donde se puede descargar la PC >	

PolicyInformation (DPC)		
policyIdentifier	<OID Autorizado por SUSCERTE>	
cPSuri	<Dirección dónde se puede descargar la DPC>	
Firma		
Algoritmo de Firma (signatureAlgorithm)	Algoritmo Autorizado (OID de los algoritmo permitido sha512WithECDSAEncryption	
Firma(signature)	<Contenido de la Firma>	

7.10.18 Certificado Electrónico de Factura Electrónica

Los certificados de factura electrónica garantizan la integridad y el no rechazo de las facturas emitidas por el comprador en formato electrónico, de acuerdo con las disposiciones reglamentarias vigentes.

Factura Electrónica		
Nombre(X.509)	**Tipo de dato [Constante] < Valor >**	**Crítica (para extensiones)**
Datos del Certificado		
Versión (versión)	Entero Hexadecimal [V4] < 0x2 >(Representa la versión 4 del X.509)	
Serial (serialNumber)	Entero Hexadecimal <Asignado por la AC> (No negativo)	
Algoritmo de Firma (signature)	Algoritmo Autorizado (OID de los algoritmos permitidos sha512WithECDSAEncryption)	
Datos de Emisor (issuer)		
Nombre Común (commonName)	UTF8 <Identificación de la AC Subordinada del Proveedor de Servicios de Certificación> **(Requerido)**	

Correo Electrónico(emailAddress)	UTF8 <Correo electrónico del ente que gestiona la AC Subordinada> **(Opcional)**	
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> **(Opcional)**	
Organización (organization)	UTF8 [Sistema Nacional de Certificación Electrónica] **(Requerido)**	
Localidad(locality)	UTF8 <Dirección física del Emisor> **(Opcional)**	
Estado(state)	UTF8 <Estado en el cual se ubica el Emisor> **(Opcional)**	
País (country)	UTF8 [VE] (ISO 3166-1-alpha-2) **(Requerido)**	
Datos de Validez		
No Antes(notBefore)	Fecha (UTC) (**Requerido)**	
No Después(notAfter)	Fecha (UTC) (**Requerido)**	
Datos de Titular (subject)		
Nombre Común (commonName)	UTF8 [Nombre que identifica al Titular del servicio de factura electrónica] **(Requerido)**	
Organización (organization)	UTF8 [Nombre completo de la constitución tal cual aparece en el documento constitutivo de la empresa] **(Requerido)**	
Correo Electrónico (emailAddress)	UTF8 <Dirección de correo electrónico de contacto del Titular> **(Opcional)**	
SerialNumber (DN)	cédula de identidad (V o E), Registro Único de Información Fiscal (G o J) o Número de Pasaporte **(Requerido)**	
Departamento (organizationUnity)	UTF8<Nombre del departamento, dirección o unidad de trabajo al cual pertenece el titular>	

	(Opcional)	
Localidad(locality)	UTF8<Ciudad donde se ubica el titular> **(Opcional)**	
Estado(state)	UTF8<Estado donde se ubica el titular> **(Opcional)**	
País (country)	UTF8 [VE] (ISO 3166-1-alpha-2) **(Requerido)**	
Información de Clave Pública del Titular (subjectPublicKey)		
Algoritmo de clave pública (algorithm)	<Algoritmo Asignado>(ecdsaEncryption, dhpublicnumber,id-ecdsa, id-ecdsaPublicKey)	
Módulo(modulus)	Cadena de Octetos [521 bit] (**Requerido)**	
* Para el caso de ECDSA se exigen los siguientes Módulos		
Extensiones		
Restricciones Básicas (basicConstraints) (**Requerido)**		
Autoridad de Certificación(aC)	Booleano [false]	
Uso de la llave (keyUsage) (**Requerido)**		
Firma digital	digitalSignature(0)	
Compromiso de contenido(contentCommitment)	contentCommitment(1) - (No Repudio)	
Cifrado de Datos (dataEncipherment)	dataEncipherment(3)	
Identificador de clave de Autoridad Certificadora (Authority Key Identifier) (Opcional)		
Clave de Autoridad(keyIdentifier)	KeyIdentifier <Identificador de la clave pública de la AC Raíz>	
Usos Extendidos de la Clave (extKeyUsage) (Opcional)		
Autenticación del servidor	id-kp-clientAuth [RFC5280]	
Protección de correo	id-kp-emailProtection[RFC5280]	

electrónico		
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		
Puntos de Distribución de las LCR (cRLDistributionPoints) (Requerido)		
Punto de distribución LCR (distributionPoint)	<Dirección de descarga de la LCR del repositorio del PSC>	
AIA (authorityInfoAccess) (Requerido)		
Método de Acceso (accessMethod)	1.3.6.1.5.5.7.48.1 [OCSP]	
Dirección de Acceso (accessLocation)	<Dirección del servicio del OCSP del PSC>	
Políticas de Certificación (PolicyInformation) (opcional)		
PolicyInformation (PC)		
policy identifier(s)	< OID Autorizado por SUSCERTE>	
cPSuir	<Dirección donde se puede descargar la PC >	
PolicyInformation (DPC)		
policyIdentifier	<OID Autorizado por SUSCERTE>	
cPSuri	<Dirección dónde se puede descargar la DPC>	

Firma		
Algoritmo de Firma (signatureAlgorithm)	Algoritmo Autorizado (OID de los algoritmos permitidos sha512WithECDSAEncryption)	
Firma(signature)	<Contenido de la Firma>	

7.10.19 Estructura Certificado Electrónico de Firma de Software

Un Certificado de Firma de Software certifica que una persona natural o jurídica es responsable del diseño, programación, mantenimiento, distribución de cualquier software, aplicación, código fuente o código objeto, así como de ser el autor de mensajes de datos que contengan información sobre ese software.

Firma de Software		
Nombre(X.509)	**Tipo de dato [Constante] < Valor >**	**Crítica (para extensiones)**
Datos del Certificado		
Versión (versión)	Entero Hexadecimal [V4] < 0x2 >(Representa la versión 4 del X.509)	
Serial (serialNumber)	Entero Hexadecimal <Asignado por la AC> (No negativo)	
Algoritmo de Firma (signature)	Algoritmo Autorizado (OID de los algoritmo permitido sha512WithECDSAEncryption)	
Datos de Emisor (issuer)		
Nombre Común (commonName)	UTF8 <Identificación de la AC Subordinada del Proveedor de Servicios de Certificación> **(Requerido)**	
Correo Electrónico(emailAddress)	UTF8 <Correo electrónico del ente que gestiona la AC Subordinada> **(Opcional)**	
Teléfono	UTF8 <Teléfono de contacto del Titular>	

(telephoneNumber)	**(Opcional)**	
Departamento (organizationUnity)	UTF8 <Nombre o razón social tal cual aparezca en el documento constitutivo del ente que gestiona la AC Subordinada> **(Opcional)**	
Organización (organization)	UTF8 [Sistema Nacional de Certificación Electrónica] **(Requerido)**	
Localidad(locality)	UTF8 <Dirección física del Emisor> **(Opcional)**	
Estado(state)	UTF8 <Estado en el cual se ubica el Emisor> **(Opcional)**	
País (country)	UTF8 [VE] (ISO 3166-1-alpha-2) **(Requerido)**	
Datos de Validez		
No Antes(notBefore)	Fecha (UTC) (**Requerido)**	
No Después(notAfter)	Fecha (UTC) (**Requerido)**	
Datos de Titular (subject)		
Nombre Común (commonName)	UTF8 [Nombre que identifica al Titular del servicio de firma de software] **(Requerido)**	
Organización (organization)	UTF8 [Nombre completo de la persona jurídica tal cual aparece en el documento constitutivo de la empresa suscriptora] **(Requerido)**	
Correo Electrónico (emailAddress)	UTF8 <Dirección de correo electrónico de contacto del Titular> **(Opcional)**	
SerialNumber (DN)	cédula de identidad (V o E), Registro Único de Información Fiscal (G o J) o Número de Pasaporte **(Requerido)**	
Departamento (organizationUnity)	UTF8<Nombre del departamento, dirección o unidad de trabajo al cuál pertenece el titular> **(Opcional)**	
Localidad(locality)	UTF8<Ciudad donde se ubica el titular o suscriptor	

	del certificado> **(Opcional)**	
Estado(state)	UTF8<Estado donde se ubica el titular o suscriptor del certificado> **(Opcional)**	
País (country)	UTF8 [VE] (ISO 3166-1-alpha-2) **(Requerido)**	
Información de Clave Pública del Titular (subjectPublicKey)		
Algoritmo de clave pública (algorithm)	<Algoritmo Asignado> (ecdsaEncryption, dhpublicnumber,id-ecdsa, id-ecdsaPublicKey)	
Módulo(modulus)	Cadena de Octetos [521 bit] (**Requerido)**	
* Para el caso de ECDSA se exigen los siguientes módulos		
Extensiones		
Restricciones Básicas (basicConstraints) (Requerido)		
Autoridad de Certificación(aC)	Booleano [false]	
Uso de la llave (keyUsage) (Requerido)		
Firma digital	digitalSignature(0)	
Compromiso de contenido(contentCommitment)	contentCommitment(1) - (No Repudio)	
Cifrado de Datos (dataEncipherment)	dataEncipherment(3)	
Identificador de clave de Autoridad Certificadora (Authority Key Identifier) (Opcional)		
Clave de Autoridad(keyIdentifier)	KeyIdentifier <Identificador de la clave pública de la AC Raíz>	
Usos Extendidos de la Clave (extKeyUsage) (Opcional)		
Autenticación del servidor	id-kp-clientAuth [RFC5280]	
Protección de correo	id-kp-emailProtection[RFC5280]	

electrónico		
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		
Puntos de Distribución de las LCR (cRLDistributionPoints) (Requerido)		
Punto de distribución LCR (distributionPoint)	<Dirección de descarga de la LCR del repositorio del PSC>	
AIA (authorityInfoAccess) (Requerido)		
Método de Acceso (accessMethod)	1.3.6.1.5.5.7.48.1 [OCSP]	
Dirección de Acceso (accessLocation)	<Dirección del servicio del OCSP del PSC>	
Políticas de Certificación (PolicyInformation) (Opcional)		
PolicyInformation (PC)		
policy identifier(s)	< OID Autorizado por SUSCERTE>	
cPSuir	<Dirección donde se puede descargar la PC >	
PolicyInformation (DPC)		
policyIdentifier	<OID Autorizado por SUSCERTE>	
cPSuri	<Dirección dónde se puede descargar la DPC>	

Firma		
Algoritmo de Firma (signatureAlgorithm)	Algoritmo Autorizado (OID de los algoritmo permitido sha512WithECDSAEncryption	
Firma(signature)	<Contenido de la Firma>	

7.10.20 Estructura Certificado Electrónico para Redes Virtuales Privadas (VPN)

Las credenciales de VPN autentican a las persona natural o jurídica, ante las redes privadas, para virtualizar, acreditar el control y propiedad de una red privada o de una máquina específica en dicha red.

Redes Virtuales Privadas (VPN)		
Nombre(X.509)	**Tipo de dato [Constante] < Valor >**	**Crítica (para extensiones)**
Datos del Certificado		
Versión (versión)	Entero Hexadecimal [V4] < 0x2 >(Representa la versión 4 del X.509)	
Serial (serialNumber)	Entero Hexadecimal <Asignado por la AC> (No negativo)	
Algoritmo de Firma (signature)	Algoritmo Autorizado (OID de los algoritmo permitido sha512WithECDSAEncryption)	
Datos de Emisor (issuer)		
Nombre Común (commonName)	UTF8 <Identificación de la AC Subordinada del Proveedor de Servicios de Certificación> **(Requerido)**	
Correo Electrónico (emailAddress)	UTF8 <Correo electrónico del ente que gestiona la AC Subordinada> **(Opcional)**	
Teléfono (telephoneNumber)	UTF8 <Teléfono de contacto del Titular> **(Opcional)**	
Departamento	UTF8 <Nombre o razón social tal cual aparezca en	

(organizationUnity)	el documento constitutivo del ente que gestiona la AC Subordinada> **(Opcional)**	
Organización (organization)	UTF8 [Sistema Nacional de Certificación Electrónica] **(Requerido)**	
Localidad(locality)	UTF8 <Dirección física del Emisor> **(Opcional)**	
Estado(state)	UTF8 <Estado en el cual se ubica el Emisor> **(Opcional)**	
País (country)	UTF8 [VE] (ISO 3166-1-alpha-2) **(Requerido)**	
Datos de Validez		
No Antes(notBefore)	Fecha (UTC) (**Requerido)**	
No Después(notAfter)	Fecha (UTC) (**Requerido)**	
Datos de Titular (subject)		
Nombre Común (commonName)	UTF8 [Nombre que identifica el servicio de Dominio o Dirección IP] **(Requerido)**	
Organización (organization)	UTF8 [Nombre de la división o departamento responsable de la VPN] **(Requerido)**	
Correo Electrónico (emailAddress)	UTF8 <Dirección de correo electrónico> **(Opcional)**	
Departamento (organizationUnity)	UTF8<Nombre del departamento o unidad organizativa> **(Opcional)**	
Localidad(locality)	UTF8<Ciudad donde se ubica el titular del certificado> **(Opcional)**	
Estado(state)	UTF8<Estado donde se ubica el titular>**<Opcional>**	
País (country)	UTF8 [VE] (ISO 3166-1-alpha-2) **(Requerido)**	
SerialNumber (DN)	cédula de identidad (V o E)	
Información de Clave Pública del Titular (subjectPublicKey)		

Algoritmo de clave pública (algorithm)	<Algoritmo Asignado>(ecdsaEncryption, dhpublicnumber,id-ecdsa, id-ecdsaPublicKey)	
Módulo(modulus)	Cadena de Octetos [521 bit] (**Requerido)**	
* Para el caso de ECDSA se exigen los siguientes módulos		
Extensiones		
Restricciones Básicas (basicConstraints) (Requerido)		
Autoridad de Certificación(aC)	Booleano [false]	
Uso de la llave (keyUsage) (Requerido)		
Firma digital	digitalSignature(0)	
Compromiso de contenido(contentCommitment)	contentCommitment(1) - (No Repudio)	
Cifrado de Datos (dataEncipherment)	dataEncipherment(3)	
Identificador de clave de Autoridad Certificadora (Authority Key Identifier) (Opcional)		
Clave de Autoridad(keyIdentifier)	KeyIdentifier <Identificador de la clave pública de la AC Raíz>	
Usos Extendidos de la Clave (extKeyUsage) (Opcional)		
Autenticación del servidor	id-kp-clientAuth [RFC5280]	
Protección de correo electrónico	id-kp-emailProtection[RFC5280]	
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		
Puntos de Distribución de las LCR (cRLDistributionPoints) (Requerido)		
Punto de distribución LCR (distributionPoint)	<Dirección de descarga de la LCR del repositorio del PSC>	
AIA (authorityInfoAccess) (Requerido)		
Método de Acceso (accessMethod)	1.3.6.1.5.5.7.48.1 [OCSP]	
Dirección de Acceso (accessLocation)	<Dirección del servicio del OCSP del PSC>	
Políticas de Certificación (PolicyInformation) (Opcional)		
PolicyInformation (PC)		
policy identifier(s)	< OID Autorizado por SUSCERTE>	
cPSuir	<Dirección donde se puede descargar la PC >	
PolicyInformation (DPC)		
policyIdentifier	<OID Autorizado por SUSCERTE>	
cPSuri	<Dirección dónde se puede descargar la DPC>	
Firma		
Algoritmo de Firma (signatureAlgorithm)	Algoritmo Autorizado (OID de los algoritmos permitidos mínimo sha512WithECDSAEncryption)	
Firma(signature)	<Contenido de la Firma>	

7.10.21 Certificado Electrónico SSL (Secure Sockets Layer).

Un certificado SSL es aquel que solicita una persona jurídica para autenticar la identidad de un sitio web y habilitar una conexión cifrada.

Certificado Electrónico SSL		
Nombre(X.509)	**Tipo de dato [Constante] < Valor >**	**Crítica (para extensiones)**
Datos del Certificado		
Versión (versión)	Entero Hexadecimal [V4] < 0x2 >(Representa la versión 4 del X.509)	
Serial (serialNumber)	Entero Hexadecimal <Asignado por la AC> (No negativo)	
Algoritmo de Firma (signature)	Algoritmo Autorizado (OID de los algoritmo permitido sha512WithECDSAEncryption)	
Datos de Emisor (issuer)		
Nombre Común (commonName)	UTF8 <Identificación de la AC Subordinada del Proveedor de Servicios de Certificación> **(Requerido)**	
Correo Electrónico(emailAddress)	UTF8 <Correo electrónico del ente que gestiona la AC Subordinada> **(Opcional)**	
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> **(Opcional)**	
Organización (organization)	UTF8 [Sistema Nacional de Certificación	

	Electrónica] **(Requerido)**	
Localidad(locality)	UTF8 <Dirección física del Emisor> **(Opcional)**	
Estado(state)	UTF8 <Estado en el cual se ubica el Emisor> **(Opcional)**	
País (country)	UTF8 [VE] (ISO 3166-1-alpha-2) **(Requerido)**	
Datos de Validez		
No Antes(notBefore)	Fecha (UTC) (**Requerido)**	
No Después(notAfter)	Fecha (UTC) (**Requerido)**	
Datos de Titular (subject)		
Nombre Común (commonName)	Dominio o dirección IP **(Requerido)**	
Organización (organization)	UTF8 [Nombre completo de la persona jurídica tal cual aparece en el documento constitutivo de la empresa suscriptora] **(Requerido)**	
Correo Electrónico (emailAddress)	UTF8 <Dirección de correo electrónico de contacto del Titular> **(Opcional)**	
Departamento (organizationUnity)	UTF8<Nombre del departamento o unidad de trabajo al cual pertenece el SSL> **(Opcional)**	
Localidad(locality)	UTF8<Ciudad donde se ubica el titular o suscriptor del certificado> **(Opcional)**	
Estado(state)	UTF8<Estado donde se ubica el titular del certificado> **<Opcional>**	
País (country)	UTF8 [VE] (ISO 3166-1-alpha-2) **(Requerido)**	
Información de Clave Pública del Titular (subjectPublicKey)		
Algoritmo de clave pública (algorithm)	<Algoritmo Asignado>(ecdsaEncryption, dhpublicnumber,id-ecdsa, id-ecdsaPublicKey)	
Módulo(modulus)	Cadena de Octetos [521 bit] (**Requerido)**	
* Para el caso de ECDSA se exigen los siguientes Módulos		
Extensiones		

Restricciones Básicas (basicConstraints) (**Requerido)**		
Autoridad de Certificación(aC)	Booleano [false]	
Uso de la llave (keyUsage) (**Requerido)**		
Firma digital	digitalSignature(0)	
Compromiso de contenido(contentCommitment)	contentCommitment(1) - (No Repudio)	
Cifrado de Datos (dataEncipherment)	dataEncipherment(3)	
Identificador de clave de Autoridad Certificadora (Authority Key Identifier) (Opcional)		
Clave de Autoridad(keyIdentifier)	KeyIdentifier <Identificador de la clave pública de la AC Raíz>	
Usos Extendidos de la Clave (extKeyUsage) (Opcional)		
Autenticación del servidor	id-kp-clientAuth [RFC5280]	
Protección de correo electrónico	id-kp-emailProtection[RFC5280]	
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		
Puntos de Distribución de las LCR (cRLDistributionPoints) (Requerido)		
Punto de distribución LCR (distributionPoint)	<Dirección de descarga de la LCR del repositorio del PSC>	
AIA (authorityInfoAccess) (Requerido)		
Método de Acceso (accessMethod)	1.3.6.1.5.5.7.48.1 [OCSP]	
Dirección de Acceso (accessLocation)	<Dirección del servicio del OCSP del PSC>	
Políticas de Certificación (PolicyInformation) (Opcional)		
PolicyInformation (PC)		
policy identifier(s)	< OID Autorizado por SUSCERTE>	
cPSuir	<Dirección donde se puede descargar la PC >	
PolicyInformation (DPC)		
policyIdentifier	<OID Autorizado por SUSCERTE>	
cPSuri	<Dirección dónde se puede descargar la DPC>	
Firma		
Algoritmo de Firma (signatureAlgorithm)	Algoritmo Autorizado (OID de los algoritmos permitidos sha512WithECDSAEncryption)	
Firma(signature)	<Contenido de la Firma>	