INFRAESTRUCTURA NACIONAL DE CERTIFICACIÓN ELECTRÓNICA: ESTRUCTURAS, CERTIFICADOS Y LISTAS DE CERTIFICADOS REVOCADOS

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
4.1	Actualizaciones asociadas al Algoritmo de Resumen (hash) Seguro asociado al Algoritmo de de Firma Digital de Curva Elíptica (ECDSA).	Mayo 2024
4.2	Actualización de conceptos, adición de conceptos y actualización de las fechas ETSI.	Noviembre 2025

Versión del Documento: Noviembre, 2025

ÍNDICE

ELABORACIÓN	
DIRECTORIO	
NOMBRE	**CARGO**
Ing. Gerardo Gómez	Superintendente.
Ing. Kimberly Zerpa	Gerente de Estandarización, Acreditación y Fiscalización.
Ing. Kevins Rangel	Gerente de Seguridad Informática.
Abg. Mónica Lugo	Consultora Jurídica.
EDICIÓN Y REVISIÓN	
Abg. Juan Carlos Centeno, Ing. Nohely Coronado, Ing. Neiver Novoa, Ing. Alberto Rodriguez e Ing. Marcial Quevedo.	

Quien suscribe, GERARDO THEIS JAHN GÓMEZ ROMERO, en su carácter de SUPERINTENDENTE DE SERVICIOS DE CERTIFICACIÓN ELECTRÓNICA, designado mediante Resolución Nº. 242 del 22 de marzo del 2024, publicada en la Gaceta Oficial de la República Bolivariana de Venezuela Nº. 42.847 de fecha 26 de marzo de 2024, actuando de conformidad a mi cargo se **Aprueba** el contenido de la Norma SUSCERTE Nº. 032-11/25 **"INFRAESTRUCTURA NACIONAL DE CERTIFICACIÓN ELECTRÓNICA: ESTRUCTURA, CERTIFICADOS Y LISTAS DE CERTIFICADOS REVOCADOS "**

Gerardo Theis Jahn Gomez Romero

Firmado Por: Gerardo Theis Jahn Gomez Romero
Fecha: 17-11-2025 09:49:04
Razón: Firma PDF
Ubicación: Caracas
Contacto: ggomez@suscerte.gob.ve
SOFE Escritorio FIIIDT-CSICE

ING. GERARDO THEIS JAHN GÓMEZ ROMERO
SUPERINTENDENTE DE SERVICIOS DE CERTIFICACIÓN ELECTRÓNICA
Designado mediante Resolución nro. 242 del 22 de marzo de 2024, publicada en la Gaceta Oficial de la República Bolivariana de Venezuela nro. 42.847 de fecha 26 de marzo de 2024

1. OBJETO Y CAMPO DE APLICACIÓN

La presente norma establece la Infraestructura Nacional de Certificación Electrónica, los requisitos Requeridos para la emisión de certificados, la estructura mínima y valores que deben estar presente en sus campos, así mismo la lista de certificados revocados, conforme a los lineamientos establecidos por la Superintendencia de Servicios de Certificación Electrónica (SUSCERTE). Su objetivo principal es asegurar la homogeneidad, interoperabilidad y confiabilidad de todos los certificados generados y utilizados en el ecosistema de certificación electrónica nacional, siendo de fiel cumplimiento para todos los Proveedores de Servicios de Certificación (PSC) que operan bajo la acreditación de está Superintendencia.

2. REFERENCIAS NORMATIVAS

2.1. Decreto N.º 1.204 con Fuerza de Ley Sobre Mensajes de Datos y Firmas Electrónicas.

2.2. Reglamento Parcial de la Ley Sobre Mensajes de Datos y Firmas Electrónicas.

2.3. Providencia Administrativa N° 016 “Normas técnicas de la infraestructura nacional de la certificación electrónica”. Gaceta Oficial de la República Bolivariana de Venezuela Nº 38.636 de fecha 2 de marzo de 2007.

2.4. ITU-T Rec. X.509 v3 Tecnología de la Información. Sistemas abiertos Interconexión: el Directorio: Marcos para certificados de claves públicas y atributos. (2019)

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

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

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

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

2.9. 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. (Octubre 2020)

2.10. RFC 3647 Public Key Infrastructure Certificate Policy and Certification Practices Framework. (Noviembre

2003)

2.11. CA-Browser-Forum TLS BR 2.0.4: Baseline Requirements for the Issuance and Management of Publicly-Trusted TLS Server Certificates. (Mayo 2025)

2.12. ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection. Information security management systems. (Febrero 2022)

2.13. ISO/IEC 27002:2022 Information security, cybersecurity and privacy protection. Information security controls. (Febrero 2022)

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

2.15. RFC 6960 X.509 Internet Public Key Infrastructure Online Certificate Status Protocol – OCSP. (Junio 2013)

2.16. RFC X.509 Certificate General-Purpose Extended Key Usage (EKU) for Document Signing. (Diciembre 2022)

2.17. CA-Browser-Forum Baseline Requirements for the Issuance and Management of Publicly-Trusted Code Signing Certificates. (Agosto 2024)

2.18. CA-Browser-Forum Network and Certificate System Security Requirements. (julio 2025)

2.19. CA-Browser-Forum Baseline Requirements for the Issuance and Management of Publicly-Trusted S/MIME Certificates. (octubre 2025)

3. DEFINICIONES Y TERMINOLOGÍAS

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

CASOS ESPECIALES	Son entidades de Certificación excepcionales destinadas a Proyectos de Interés Nacional que son acreditados por la Superintendencia de Servicios de Certificación Electrónica (SUSCERTE).
CERTIFICADO RAÍZ	El Certificado autofirmado emitido por la AC Raíz para identificarse y facilitar la verificación de los Certificados emitidos a sus AC Subordinadas.
CERTIFICADO ELECTRÓNICO	Mensaje de Datos proporcionado por un Proveedor de Servicios de Certificación que le atribuye certeza y validez a la Firma Electrónica.
CLAVE PÚBLICA	Es una clave matemática que tiene disponibilidad pública y que es utilizada por las aplicaciones para verificar las firmas digitales creadas con su correspondiente clave privada.
CURVA ELÍPTICA (ECDSA)	Es un enfoque de la criptografía de clave pública basado en la estructura algebraica de curvas elípticas sobre campos finitos.
DIRECCIÓN IP	Secuencia numérica que identifica de manera única y jerárquica a cada interfaz de red, esta puede ser dinámica o estática.
DN	Acrónimo de Distinguished Name (Nombre Distinguido) y es un conjunto de valores que se ingresan durante el proceso de inscripción y la creación de una solicitud de firma de certificado (CSR).
FORMATO UTC	El Tiempo Universal Coordinado por sus siglas en inglés UTC o hora civil, que es la zona horaria de referencia a partir de la cual se calculan todas las demás partes del mundo.
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.
IDENTIFICADOR DE OBJETO	Valor universal único asociado a un objeto para identificarlo inequívocamente.

ISSUER	Es la entidad que verificó la información y firmó el certificado.
LDAP	Estándar de Internet que proporciona acceso a la información desde distintas aplicaciones y sistemas informáticos. Usa un conjunto de protocolos para acceder a los directorios y recuperar la información.
LISTA DE CERTIFICADOS REVOCADOS	Documento mantenido y publicado por una Autoridad de Certificación (AC) que enumera los certificados revocados por ella.
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, incluyendo Internet.
PC	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.
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.
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.
NUMERO DE SERIE DEL CERTIFICADO (SERIAL NUMBER)	Es un número de serie que identifica de forma única el certificado, es un número entero positivo asignado por la CA de cada certificado.
ATRIBUTO DEL SUJETO (SUBJECT ATTRIBUTE: SERIALNUMBER)	El atributo serialNumber es un componente del Nombre Distinguido (`Subject Name`) del certificado X.509. Su propósito es portar el número de identificación único y oficial (como la cédula de identidad, RIF, Pasaporte) del titular, sirviendo como un identificador de identidad primario dentro de la información del sujeto.
PATROCINADOR VALIDADO (SPONSOR-VALIDATED PROFILE)	Es una validación que tiene como finalidad equilibrar la identidad de la organización Patrocinadora (que es la responsable del certificado) con la identidad del individuo que lo usa.

4. SÍMBOLOS Y ABREVIATURAS

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

CA / AC	Certification Authority /Autoridad de Certificación.
AIA	Acceso a la Información de Autoridad.
RA / AR	Registration Authority / Autoridad de Registro.
ASN.1 / NSAU	Abstract Syntax Notation One / Notación de Sintaxis Abstracta Uno.
DNS / SND	Domain Name System / Sistema de nombres de dominio.
DPC / CPS	Declaración de Prácticas de Certificación / Certification Practices Statement.
EV / VE	Extended Validation / Validación Extendida.
OV/VO	Extended Validation / Organización Validada.
DV/VD	Validated Domain / Dominio Validado.
VI/IV	Individual Validation / Validación Individual.
GSM / SGC	Global System for Mobile Communications / Sistema global para las comunicaciones móviles.
HSM / MSH	Hardware Security Module. / Módulo de Seguridad de Hardware.
PKI / ICP	Public Key Infrastructure / Infraestructura de clave pública.
IMEI	International Mobile Equipment Identity / Identidad internacional de equipo móvil.
ITU-T	International Telecommunications Union-Telecommunications / Unión Internacional de Telecomunicaciones.
LCR	Lista de Certificados Revocados.
LDAP	Lightweight Directory Access Protocol / Protocolo ligero de acceso a directorios.
LSMDFE	Ley Sobre Mensajes de Datos y Firmas Electrónicas.
MAC	Media Access Control / Control de acceso al medio.
OCSP	Online Certificate Status Protocol / Protocolo de estado de certificados en línea.
OID	Object Identifier / Identificador de Objeto.
PC	Política de Certificados.
SAN	SubjectAlternativeName/Nombre alternativo del sujeto.
PSC	Proveedor de Servicios de Certificación.
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	Unstructured Supplementary Service Data / Servicio suplementario de datos no estructurados.

5. PROCEDIMIENTO

5.1 Consideraciones Generales

5.1.1 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.

5.1.2 La Infraestructura Nacional de Certificación Electrónica, estará sujeto a un modelo jerárquico, SUSCERTE es la Autoridad de Certificación Raíz única nacional, toda acreditación emitida por él, deberá estar adecuada a su normativa.

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

5.1.4 En la Figura Nº 1 se ilustra la arquitectura jerárquica donde la confianza emanada de SUSCERTE, como única Autoridad de Certificación AC Raíz, es la fuente innegable de autenticidad, centralizando la seguridad y validando a todas las demás autoridades de certificación subordinadas, garantizando que cada certificado emitido posee una cadena de confianza ininterrumpida y verificable, protegiendo la integridad y el no repudio.

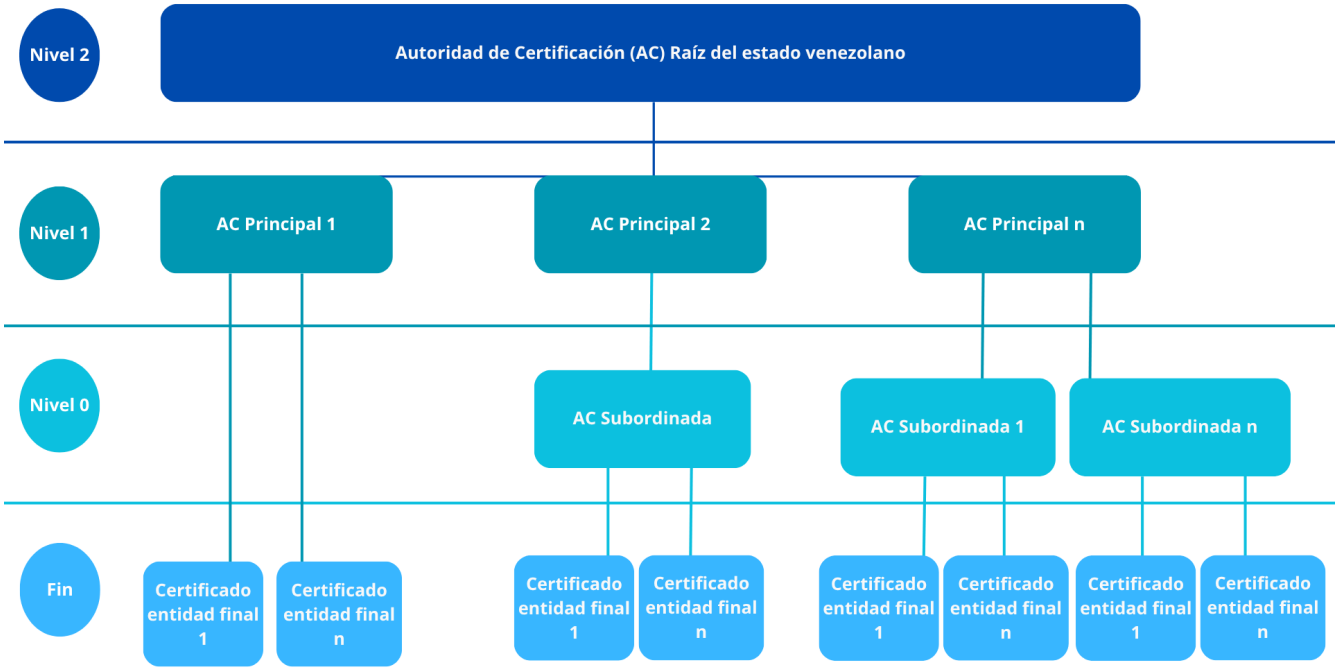

Figura 1 *Modelo de Jerarquía*

5.1.5 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, más no pueden emitir certificados a su AC superior.

5.1.6 En la arquitectura jerárquica de la Infraestructura Nacional de Certificación Electrónica, el ente rector autorizará que los PSC constituyan por debajo de ellos un solo nivel de AC subordinadas.

5.1.7 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 las AC subordinadas se ve comprometida no afectará a las otras.

5.1.8 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.

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

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

5.1.11.1 Los PSC 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.

5.1.11.2 La AC Raíz autoriza las AC subordinadas que el PSC solicite, estás solo podrán emitir certificados a los suscriptores.

5.1.12 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, informando al signatario las obligaciones que asume cuando adquieren un certificado, 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 un tercero, previa validación de la identidad de estos y del suscriptor, por la autoridad que expide el certificado, tendrán a su disposición el certificado electrónico mediante el uso de dispositivos criptográficos, entre otros.

c) **Certificados para Sistemas:** Serán usados por software, 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.

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

5.3.5 Los PSC deben cumplir con los perfiles de certificados establecido en la presente Norma, en el caso de solicitar la incorporación de nuevos perfiles de certificados, estos deberán ser sometidos a consideración, evaluación y aprobación por parte de SUSCERTE.

5.3.6 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)	25 años	521
AC Principal PSC		10 años	384 o 521
AC Subordinada PSC		9 años	384 o 521
AC Caso Especial		Depende del caso	384 o 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	256
	Hardware (token criptográfico, tarjeta inteligente)	Depende del caso	256
Para software o aplicaciones	Software	Depende del caso	256
	Hardware (HSM)	Depende del caso	256

Tabla Nº 1

5.3.7 Es Requerido el uso de HSM fisico para el almacenamiento del par de claves de los certificados de la AC Raíz, AC Principal del PSC, AC Subordinadas y AC Caso Especial.

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

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

5.3.10 El signatario y suscriptor deben conocer las políticas de uso de los certificados electrónicos establecidas por el PSC, para las buenas prácticas y el uso permitido de los mismos. Para ello, el PSC deberá promover que los signatarios y suscriptores conozcan dichas políticas. En caso de solicitud de un certificado electrónico 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.509 v3, 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, Número de Serie 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 Numero de serie (serialNumber)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 ni cero. Su valor es un número entero grande.

5.4.4.1 El Numero de serie (serialNumber) en Datos del Subject (Atributo del DN), se utiliza para incluir un número de identificación legal, gubernamental o de registro de la entidad a la que pertenece el

certificado. El valor es una cadena de caracteres que representa un identificador oficial.

5.4.5 Para los certificados Electrónicos de AC la longitud de cifrado puede ser de NIST P-384 o NIST P-521, haciendo uso del algoritmo de firma sha384 o 512WithECDSAEncryption según sea el caso de uso. En el caso de los Certificados Electrónicos de Entidad Final la longitud de cifrado puede variar entre NIST P-256, NIST P-384 o NIST P-521, haciendo uso del algoritmo de firma sha256, sha384 o 512WithECDSAEncryption.

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 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 vigente en la Tabla N° 1.

5.4.9 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..

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

5.4.11 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.

5.4.12 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) y Acceso a la Información de Autoridad (authorityInfoAccess, AIA).

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

5.4.14 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 de 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“.

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

5.4.16 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.

5.4.17 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).

5.4.18 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).

5.4.19 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).

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

5.4.21 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.

5.4.22 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.

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

5.4.24 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.

5.4.25 Todo campo que no esté clasificado en la estructura del certificado como opcional, es Requerido.

5.4.26 En caso de que el PSC o Caso Especial estimen en sus políticas de certificados, campos adicionales a los Requeridos 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.

5.4.27 En caso de que el PSC o Caso Especial estimen en sus políticas de certificados campos adicionales a los Requeridos 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 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 debe modificar su normativa y solicitará 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 el portal web de Suscerte: https://www.suscerte.gob.ve , se deberá iniciar por parte de los Proveedores de Servicios de Certificación, la actualización de sus políticas de certificación y los perfiles de los certificados electrónicos que hayan sido modificados.

SEGUNDA: Los PSC tendrán un período de seis (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 implementación de los cambios de actualización por parte del PSC, SUSCERTE deberá realizar una inspección, para validar las buenas prácticas de certificación.

7. ANEXOS

Los anexos son parte integrante de la presente norma y deben ser de cumplimiento Requerido por parte de los PSC.

7.1 Anexo A: Uso del *DN serialNumber (Titular [Subject])*

- Se debe utilizar para identificar únicamente al emisor y titular del certificado electrónico.
- Para identificar personas se debe utilizar la Cédula de Identidad o Número de Pasaporte y Registro Único de Información Fiscal (R.I.F).
- 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: V00000000 o E00000000, según sea el caso.
- El Pasaporte deberá incluir todos los dígitos de dicho documento.
- Para identificar organismos 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: V00000000, G00000000, J000000000, C000000000, P000000000.
- Para identificar dispositivos, sistemas o componentes de sistemas, 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.
- SUSCERTE podrá asignar y autorizar la utilización de Identificador de Objeto Único (OID) para distinguir al PSC.

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	organizationName	2.5.4.10
Departamento	organizationalUnitName	2.5.4.11
País	countryName	2.5.4.6
Correo Electrónico	emailAddress	1.2.840.113549.1.9.1
Localidad	localityName	2.5.4.7
Estado	stateOrProvinceName	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

Nombre	X.509	O.I.D.
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

La extensión Usos Extendidos de Clave (Extended Key Usage o EKU), definida en el estándar X.509 v3, especifica uno o más propósitos adicionales o más específicos para los que la clave pública contenida en el certificado puede ser utilizada. Esta extensión es fundamental para limitar y definir el alcance de un certificado digital.

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	secureShellClient	1.3.6.1.5.5.7.3.21
Secure Shell Authentication Server	secureShellServer	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

Nota Importante sobre OIDs: Los OIDs que comienzan con `1.3.6.1.5.5.7.3` son definidos por los estándares de PKIX (RFC 5280 y posteriores), mientras que los que empiezan por `1.3.6.1.4.1.311` son privados de Microsoft y se usan en entornos Windows. El OID de Adobe es de uso propietario para la firma de documentos PDF.

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

La CRL es el elemento de gestión de revocación.

Perfil de Lista de Certificados Revocados		
Nombre(LCR/CRL)	**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 (*signatureAlgorithm*)	Algoritmo Autorizado (OID de los algoritmo permitido sha512WithECDSAEncryption)	
Datos de Emisor (*issuer*)		
Nombre Común (*commonName*)	UTF8 <Identificación de la AC emisora> **(Requerido)**	
Departamento (*organizationalUnitName*)	UTF8 <Nombre o unidad del departamento que pertenece el emisor> **(Opcional)**	
Organización (*organizationName*)	UTF8 [Sistema Nacional de Certificación Electrónica] **(Requerido)**	
Localidad (*localityName*)	UTF8 <Dirección física del emisor> **(Opcional)**	
Estado (*stateOrProvinceName*)	UTF8 <Estado en el cual se ubica el emisor> **(Opcional)**	
País (*countryName*)	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) (Requerido)		
Clave de Autoridad (*keyIdentifier*)	*KeyIdentifier* <Identifica la clave de la CA que firma la CRL> **(Requerido)**	
Numero de LCR (CRL Number) (Requerido)		
Número de serie del certificado (CertificateSerialNumber)	*CertificateSerialNumber* <Contiene el número de LCR emitidos> **(Requerido)**	

Uso de la llave (keyUsage) (Opcional)		
Firma de LCR	cRLSign (Bit 6)	
Puntos de Distribución de las LCR (*IssuingdistributionPoint*)		x
Punto de distribución LCR (*distributionPoint*)	<Dirección de descarga de la LCR por el PSC> **(Requerido)**	
Punto de Distribución de la CRL más Fresca (Freshest CRL) RFC 5280		
FreshestCRL	Id-ce-freshestCRL <Identifica donde se puede obtener la LCR delta (listas más pequeñas que contienen los certificados revocados desde la ultima LCR Base)>	
Certificados Revocados		
Certificados revocados (Revoked Certificates)		
Serial del Certificado (*Serial Number*)	Entero Hexadecimal<Serial de certificado revocado > **(Requerido)**	
Fecha de revocación (*RevocatiónDate*)	Fecha<fecha y hora en formato UTC> **(Requerido)**	
Razón de Revocación (*CRL ReasonCode*)	Razón de Revocación < Indicar la razón específica de la revocación. Ver Anexo G > **(Requerido)**	
Firma		
Algoritmo de Firma (*signatureAlgorithm*)	Algoritmo Autorizado (OID de los algoritmo permitido sha512WithECDSAEncryption)	
Firma(*signature*)	<Contenido de la Firma>	

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 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 Electrónicos

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 [V3] < 0x2 >(Representa la versión 3 del X.509) **(Requerido)**	
Serial (S*erial Number*)	Entero Hexadecimal <Asignado por la AC> (No negativo) **(Requerido)**	
Algoritmo de Firma (*signatureAlgorithm*)	Algoritmo Autorizado (OID de los algoritmo permitido sha384/512WithECDSAEncryption)	
Datos de Emisor (*issuer*)		
Nombre Común (*commonName*)	UTF8 [SUSCERTE] **(Requerido)**	
Organización (*organizationName*)	UTF8 [Sistema Nacional de Certificación Electrónica] **(Requerido)**	
País (*countryName*)	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 (*organizationName*)	UTF8 [Sistema Nacional de Certificación Electrónica] **(Requerido)**	
País (*countryName*)	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)	
NIST CURVE	P-384/521	
Para el caso de ECDSA se exigen los módulos anteriores		
Extensiones		
Restricciones Básicas (basicConstraints) **(Requerido)**		**X**

Autoridad de Certificación(aC)	Booleano [true]	
Identificador de la clave del titular (Subject Key Identifier) **(Requerido)**		
Clave de Autoridad (*keyIdentifier*)	KeyIdentifier <clave pública del propio certificado de la AC Subordinada> **(Requerido)**	
Identificador de clave de Autoridad Certificadora (Authority) (Requerido)		
Clave de Autoridad (*keyIdentifier*)	KeyIdentifier <el valor del keyIdentifier debe ser idéntico al **SKI** de la Raíz> **(Requerido)**	
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 sha384/512WithECDSAEncryption)	
Firma(*signature*)	<Contenido de la Firma>	

7.10.2 Estructura de Certificado de la 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 Subordinada del PSC		
Nombre(X.509)	**Tipo de dato [Constante] < Valor > (Observación)**	**Crítica (para extensiones)**
Datos del Certificado		
Versión (versión)	Entero Hexadecimal [V3] < 0x2 >(Representa la versión 3 del X.509) (Requerido)	
Serial (S*erial Number*)	Entero Hexadecimal <Asignado por la AC> (No negativo)**(Requerido)**	
Algoritmo de Firma (*signatureAlgorithm*)	Algoritmo Autorizado (OID de los algoritmos permitidos mínimo sha384/512WithECDSAEncryption) **(Requerido)**	
Datos de Emisor (*issuer*)		
Nombre Común (*commonName*)	UTF8 [SUSCERTE] **(Requerido)**	

Organización (*organizationName*)	UTF8 [Sistema Nacional de Certificación Electrónica] **(Requerido)**	
País (*countryName*)	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 <El nombre específico de la CA principal> **(Requerido)**	
Departamento (*organizationalUnitName*)	UTF8 <Nombre de la división interna que opera(ej., Certificados PKI)> **(Opcional)**	
Organización (*organizationName*)	UTF8 [Sistema Nacional de Certificación Electrónica] **(Requerido)**	
Localidad (*localityName*)	UTF8<Información de la localidad de la AC> (Opcional)	
Estado (*stateOrProvinceName*)	UTF8 <Información del estado o provincia de la AC> **(Opcional)**	
País (*countryName*)	UTF8 [VE] (ISO 3166-1-alpha-2) **(Requerido)**	
Información de Clave Pública del Titular		
Algoritmo de clave pública (*algorithm*)	<Algoritmo Asignado> (ecdsaEncryption, dhpublicnumber,id-ecdsa, id-ecdsaPublicKey)	
NIST CURVE	P-*nnn* donde *nnn* puede ser 384 o 521 **(Requerido)** Aplicar según la curva indicada en la longitud de la firma seleccionada en el "Algoritmo de Firma (*signatureAlgorithm*)	
*** 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)**	
Identificador de la clave del titular (Subject Key Identifier) (Requerido)		
Clave de Autoridad (*keyIdentifier*)	KeyIdentifier <clave pública del propio certificado de la AC principal> **(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) (Requerido)		
Clave de Autoridad (*keyIdentifier*)	KeyIdentifier <Debe ser una copia del **Subject Key Identifier (SKI)** del certificado de la CA Superior que firmó la AC principal> **(Requerido)**	
Puntos de Distribución de las LCR (cRLDistributionPoints) (Requerido)		
Punto de distribución LCR (*distributionPoint*)	<URL HTTP del servicio CRL de la AC>	
AIA (authorityInfoAccess) (Requerido)		
id-ad-ocsp	1.3.6.1.5.5.7.48.1 <URL HTTP del respondedor OCSP de la CA emisora (accessLocation)> (opcional)	
id-ad-caIssuers	1.3.6.1.5.5.7.48.2 <URL HTTP del certificado de la CA emisora (accessLocation)> (opcional, pero debería)	
PolicyIdentifier (PC/CP) (Requerido)		
PolicyQualifiers (DPC/CPS) (Requerido)		
cPSuri	<URL de la Declaración de Prácticas de Certificación (CPS) de la CA emisora>	
Firma		
Algoritmo de Firma (*signatureAlgorithm*)	Algoritmo Autorizado (OID de los algoritmos permitidos mínimo sha512WithECDSAEncryption)	
Firma(signature)	<Contenido de la Firma>	

7.10.3 Estructura de Certificado de la 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 [V3] < 0x2 >(Representa la versión 3 del X.509) (Requerido)	
Serial (S*erial Number*)	Entero Hexadecimal <Asignado por la AC> (No negativo)**(Requerido)**	
Algoritmo de Firma (*signatureAlgorithm*)	Algoritmo Autorizado (OID de los algoritmos permitidos mínimo sha384/512WithECDSAEncryption) **(Requerido)**	

Datos de Emisor (*issuer*)		
Nombre Común (*commonName*)	UTF8 <Identificación de la AC del Proveedor de Servicios de Certificación> **(Requerido)**	
Departamento (*organizationalUnitName*)	UTF8<Nombre de la división interna de la organización(ej., Gerencia de PKI)> **(Opcional)**	
Organización (*organizationName*)	UTF8 [Sistema Nacional de Certificación Electrónica] **(Requerido)**	
Localidad(*localityName*)	UTF8<Ciudad donde se ubica el PSO> **(Opcional)**	
Estado(*stateOrProvinceName*)	UTF8<Información del estado o provincia del PSC> **(Opcional)**	
País (*countryName*)	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 <El nombre específico de la CA Subordinada (ej. “AC subordinada de firma de documentos”)> **(Requerido)**	
Departamento (*organizationalUnitName*)	UTF8 <Nombre de la división interna que opera(ej., Certificados servidor)> **(Opcional)**	
Organización (*organizationName*)	UTF8 [Sistema Nacional de Certificación Electrónica] **(Requerido)**	
Localidad (*localityName*)	UTF8<Información de la localidad del emisor> (Opcional)	
Estado (*stateOrProvinceName*)	UTF8 <Información del estado o provincia del emisor> **(Opcional)**	
País (*countryName*)	UTF8 [VE] (ISO 3166-1-alpha-2) **(Requerido)**	
Información de Clave Pública del Titular		
Algoritmo de clave pública (*algorithm*)	<Algoritmo Asignado> (ecdsaEncryption, dhpublicnumber,id-ecdsa, id-ecdsaPublicKey)	
NIST CURVE	P-*nnn* donde *nnn* puede ser 384 o 521 **(Requerido)** Aplicar según la curva indicada en la longitud de la firma seleccionada en el “Algoritmo de Firma (*signatureAlgorithm*)	
*** 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)**	
Identificador de la clave del titular (Subject Key Identifier) (Requerido)		
Clave de Autoridad (*keyIdentifier*)	KeyIdentifier <clave pública del propio certificado de la AC Subordinada> **(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) (Requerido)		
Clave de Autoridad (*keyIdentifier*)	KeyIdentifier <Debe ser una copia del **Subject Key Identifier (SKI)** del certificado de la CA Superior que firmó la AC Subordinada> **(Requerido)**	
Puntos de Distribución de las LCR (cRLDistributionPoints) (Requerido)		
Punto de distribución LCR (*distributionPoint*)	<URL HTTP del servicio CRL de la AC>	
AIA (authorityInfoAccess) (Requerido)		
id-ad-ocsp	1.3.6.1.5.5.7.48.1 <URL HTTP del respondedor OCSP de la CA emisora (accessLocation)> (opcional)	
id-ad-caIssuers	1.3.6.1.5.5.7.48.2 <URL HTTP del certificado de la CA emisora (accessLocation)> (opcional, pero debería)	
PolicyIdentifier (PC/CP) (Requerido)		
PolicyQualifiers (DPC/CPS) (Requerido)		
cPSuri	<URL de la Declaración de Prácticas de Certificación (CPS) de la CA emisora>	
Firma		
Algoritmo de Firma (*signatureAlgorithm*)	Algoritmo Autorizado (OID de los algoritmos permitidos mínimo sha512WithECDSAEncryption)	
Firma(signature)	<Contenido de la Firma>	

7.10.4 Estructura de Certificado Electrónico para Servidor de OCSP

Emitido para firmar respuestas generadas del servicio OCSP de una AC. El servidor OCSP toma una solicitud y genera una respuesta firmada digitalmente por el emisor (el certificado de OCSP Responder).

Certificado de Servidor de OCSP

Nombre(X.509)	Tipo de dato [Constante] < Valor >	Crítica (para extensiones)
Datos del Certificado		
Versión (versión)	Entero Hexadecimal [V3] < 0x2 >(Representa la versión 3 del X.509) (Requerido)	
Serial (*Serial Number*)	Entero Hexadecimal <Asignado por la AC> (No negativo) **(Requerido)**	
Algoritmo de Firma (*signatureAlgorithm*)	Algoritmo Autorizado (OID de los algoritmo permitido sha256/384/512WithECDSAEncryption)	
Datos de Emisor (*issuer*)		
Nombre Común (*commonName*)	UTF8 < "UTF8 [identificación de la AC principal O Subordinada] **(Requerido)**	
Departamento (*organizationalUnitName*)	UTF8 <División o unidad de la CA (ej. "Departamento de Emisión de Certificados"> **(Opcional)**	
Organización (*organizationName*)	UTF8 [Sistema Nacional de Certificación Electrónica] **(Requerido)**	
Localidad(*localityName*)	UTF8 <Dirección física del Emisor> **(Opcional)**	
Estado (*stateOrProvinceName*)	UTF8 <Estado en el cual se ubica el Emisor> **(Opcional)**	
País (*countryName*)	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 de manera clara el servicio (ej. OCSP Responder AC emisora)] **(Requerido)**	
Departamento (*organizationalUnitName*	UTF8<Nombre de la división interna de la organización(ej., Gerencia de PKI)> **(Opcional)**	
Organización (*organizationName*)	UTF8 <El nombre legal de la organización que opera el servicio OCSP> **(Requerido)**	
Localidad(*localityName*)	UTF8 <La ciudad donde se encuentra el servidor o la CA.> **(Opcional)**	
Estado (*stateOrProvinceName*)	UTF8 <El estado o provincia donde se encuentra el servidor o la CA> **(Opcional)**	
País (*countryName*)	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)	

NIST CURVE	P-*nnn* donde *nnn* puede ser 256, 384 o 521 **(Requerido)** Aplicar según la curva indicada en la longitud de la firma seleccionada en el "Algoritmo de Firma (*signatureAlgorithm*)"	
*** Para el caso de ECDSA se exigen los módulos anteriores**		
Extensiones		
Restricciones Básicas (basicConstraints) (Opcional)		
Autoridad de Certificación(aC)	Booleano [false]	
Uso de la llave (keyUsage) (Requerido)		
Firma digital	digitalSignature(0)	
Identificador de clave de Autoridad Certificadora (Authority Key Identifier) (Requerido)		
Clave de Autoridad (*keyIdentifier*)	KeyIdentifier <Identificador de la clave pública de la AC>	
Usos Extendidos de la Clave (extKeyUsage) (Requerido)		x
Firma de OCSP	ocspSigning 1.3.6.1.5.5.7.3.9	
AIA (authorityInfoAccess) (Requerido)		
id-ad-ocsp	1.3.6.1.5.5.7.48.1 <URL HTTP del respondedor OCSP de la CA emisora (accessLocation)> (opcional)	
id-ad-calssuers	1.3.6.1.5.5.7.48.2 <URL HTTP del certificado de la CA emisora (accessLocation)> (opcional, pero debería)	
Políticas de certificado (certificatePolicies)(Opcional)		
PolicyQualifiers (DPC/CPS)		
cPSuri	<URL de la Declaración de Prácticas de Certificación (CPS) de la CA emisora>	
Firma		
Algoritmo de Firma (*signatureAlgorithm*)	Algoritmo Autorizado (OID de los algoritmo permitido sha256/384/512WithECDSAEncryption)	
Firma(*signature*)	<Contenido de la Firma>	

7.10.4.1 Estructura de respuesta para servidor de OCSP

Estructura guía del respondedor OCSP, desde la solicitud al servidor.

Respondedor del servicio OCSP		
Nombre(X.509)	**Tipo de dato [Constante] < Valor >**	
Datos de solicitud OCSP (OCSP Request Data)		
Versión (versión)	<Versión del protocolo v1[0]> (RFC 6960)	
Lista de solicitantes(Requestor list) Contiene una o más solicitudes de estado de certificado individual		
Identificador del certificado a consultar (CertID)		
hashAlgorith	Es el algoritmo hash utilizado (RFC 6960)	
issuerNameHash	Hash del Nombre Distinguido (DN) del Emisor RFC (6960)	
issuerKeyHash	Hash de la Clave Pública del Emisor (RFC 6960)	
SerialNumber	Número de serie del certificado para el cual se solicita el estado.	
Datos de respuesta de OCSP (OCSP Response Data)		
Estado de respuesta OCSP(Response Status)	<Indica el proceso de la petición>	
Version (version)	<Versión de la respuesta (V1)>	
IProduced At	<La hora exacta en que el respondedor generó la respuesta.>	
Responses	<Contiene el estado de los certificados consultados (uno o más)>	
Cert Status	<El estado de revocación del certificado (good, revoked o unknown)>	
This Update	<La hora de la última actualización de la información de revocación>	
Next Update	<El momento antes del cual estado del certificado no cambiará> **(Opcional)**	
Firma		
Algoritmo de Firma (*signatureAlgorithm*)	Algoritmo Autorizado (OID de los algoritmo permitido sha256/384/512WithECDSAEncryption)	

7.10.5 Estructura de Certificado Electrónico para Persona Natural

Certificado emitido a nombre de un individuo, su propósito es permitir que esa persona se identifique de forma segura mediante firmas electrónicas con validez legal, actuando siempre en nombre propio. Este requisito implica una **verificación de identidad** que vincula la clave criptográfica directamente a la identidad legal de la persona, lo que es característico del perfil Validación Individual (VI) de SMIMEBR.

Certificado Persona Natural		
Nombre(X.509)	**Tipo de dato [Constante] <Valor> (Observación)**	**Crítica (para extensiones)**
Datos del Certificado		
Versión (versión)	Entero Hexadecimal [V3] < 0x2 >(Representa la versión 3 del X.509)	
Serial (*Serial Number*)	Entero Hexadecimal <Asignado por la AC> (No negativo)	
Algoritmo de Firma (*signatureAlgorithm*)	Algoritmo Autorizado (OID de los algoritmo permitido sha256/384/512WithECDSAEncryption)	
Datos de Emisor (issuer)		
Nombre Común (*commonName*)	UTF8 <identificación de la AC principal O Subordinada> **(Requerido)**	
Departamento (*organizationalUnitName*)	UTF8 <División o unidad de la CA (ej. "Departamento de Emisión de Certificados")> **(Opcional)**	
Organización (*organizationName*)	UTF8 [Sistema Nacional de Certificación Electrónica] **(Requerido)**	
Localidad (*localityName*)	UTF8 <Dirección física del Emisor> **(Opcional)**	
Estado (*stateOrProvinceName*)	UTF8 <Estado en el cual se ubica el Emisor> **(Opcional)**	
País (*countryName*)	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*)	<Si la CA elige colocar el nombre completo se debe seguir las directrices de la CA browser Forum BR SMIME>	
Seudónimo(Pseudonym)	<Si contiene este campo es **Requerido** contener el Alias o sobrenombre verificado, los atributos Nombre y Apellido no deben estar presentes>	
Nombre (GivenName)	<Nombre del sujeto> (Si el CN es el Nombre Personal es **Requerido** que el certificado use atributos separados, y para este caso Seudónimo no debe estar presente)	
Apellido (Surname)	<Nombre del sujeto> (Si el CN es el Nombre Personal es **Requerido** que el certificado use atributos separados, y para este caso Seudónimo no debe estar presente)	
serialNumber (DN)	Identificación fiscal o legal de la entidad **(Opcional)**	
Dirección de correo(emailAddress)	<La dirección de correo> Es O**pcional** en Subject DN, pero su presencia en la extensión SAN del presente certificado es **Requerido**	
Localidad(*localityName*)	UTF8<Ciudad donde se ubica el titular> **(Opcional)**	

Estado (*stateOrProvinceName*)	UTF8<Información del estado o provincia del titular> **(Opcional)**	
País (*countryName*)	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)	
NIST CURVE	P-*nnn* donde *nnn* puede ser 256, 384 o 521 **(Requerido)** Aplicar según la curva indicada en la longitud de la firma seleccionada en el "Algoritmo de Firma (*signatureAlgorithm*)"	
*** Para el caso de ECDSA se exigen los módulos anteriores (Requerido)**		
Extensiones		
Restricciones Básicas (basicConstraints) (Opcional)		
Autoridad de Certificación(aC)	Booleano [false]	
Uso de la llave (keyUsage)(Requerido)		x
Firma digital	DigitalSignature(0) (**Requerido)**	
Compromiso de contenido (*contentCommitment*)	contentCommitment(1) - <Antes No Repudio - compromiso con el contenido firmado> (Requerido)	
Acuerdo de claves (keyAgreement)	<Para establecer claves de sesión para cifrado del contenido del correo> (Requerido)	
Identificador de clave de Autoridad Certificadora (Authority Key Identifier) (Requerido)		
Clave de Autoridad (*keyIdentifier*)	KeyIdentifier <Identificador de la clave pública de la AC emisora> (Requerido)	
Identificador de la clave del sujeto (Subject Key Identifier) (Recomendable)RFC 5280		
Clave de Autoridad (*keyIdentifier*)	KeyIdentifier <clave pública del propio certificado de la AC>	
Nombre alternativo del sujeto (subjectAlternativeName) (Requerido)		
Formato de correo tradicional	Dirección de correo electrónico <Rfc822Name o SmtpUTF8Mailbox(RFC 9598)> (Requerido)	
Nombre del directorio (directoryname)	<GeneralName> (Opcional)	
Usos Extendidos de la Clave (extKeyUsage) (Requerido)		Definido por el emisor (RFC 5280 y RFC 9336)
Firma de documentos	Id-kp-documentSignin 1.3.6.1.4.1.311.10.3.12 (Requerido para firma de documentos)	
Protección de correo	Id-kp-emailProtection 1.3.6.1.5.5.7.3.4 (Requerido para s/mime)	
Puntos de Distribución de las LCR (cRLDistributionPoints) (Requerido)		

Punto de distribución LCR (*distributionPoint*)	<URL HTTP del servicio CRL de la AC>	
AIA (authorityInfoAccess) (Requerido)		
id-ad-ocsp	1.3.6.1.5.5.7.48.1 <URL HTTP del respondedor OCSP de la CA emisora (accessLocation)> (opcional)	
id-ad-calssuers	1.3.6.1.5.5.7.48.2 <URL HTTP del certificado de la CA emisora (accessLocation)> (opcional, pero debería)	
Políticas de certificado (certificatePolicies)(Requerido)		
PolicyIdentifier (Identificador de política) Requerido		
policy identifier(s)	<Indica la política de la CA que confirma el cumplimiento>	
PolicyQualifiers (Calificador de política)		
cPSuri	<URL de la Declaración de Prácticas de Certificación (DPC/CPS) de la CA emisora>	
Firma		
Algoritmo de Firma (*signatureAlgorithm*)	Algoritmo Autorizado (OID de los algoritmos sha256/384/512WithECDSAEncryption)	
Firma(*signature*)	<Contenido de la Firma>	

7.10.6 Estructura de Certificado Electrónico para Persona Jurídica

Certificado cuyo suscriptor es una empresa u organización y el titular es una persona natural que lo representa legalmente, destinado para firmar electrónicamente mensajes de datos, autorizados por el suscriptor. Este perfil se ajusta a la validación de Organización Validada (OV).

Certificado Persona Jurídica		
Nombre(X.509)	**Tipo de dato [Constante] < Valor > (Observaciones)**	**Crítica (para extensiones)**
Datos del Certificado		
Versión (versión)	Entero Hexadecimal [V3] < 0x2 >(Representa la versión 3 del X.509) **(Requerido)**	
Serial (S*erial Number*)	Entero Hexadecimal <Asignado por la AC> (No negativo) **(Requerido)**	
Algoritmo de Firma (*signatureAlgorithm*)	Algoritmo Autorizado (OID de los algoritmo permitido sha256/384/512WithECDSAEncryption)	
Datos de Emisor (issuer)		
Nombre Común (*commonName*)	UTF8 <identificación de la AC principal O Subordinada> **(Requerido)**	

Departamento (*organizationalUnitName*)	UTF8 <Se incluye como información de contacto adicional para la entidad firmante (persona natural o jurídica), pero no es un requisito para la validez criptográfica> **(Opcional)**	
Organización (*organizationName*)	UTF8 [Sistema Nacional de Certificación Electrónica] **(Requerido)**	
Localidad (*localityName*)	UTF8 <Dirección física del Emisor> **(Opcional)**	
Estado (*stateOrProvinceName*)	UTF8 <Estado en el cual se ubica el Emisor> **(Opcional)**	
País (*countryName*)	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 <El nombre de la entidad que firma> **(Opcional)**	
Organización (*organizationName*)	UTF8 <El nombre legal de la organización> **(Requerido)**	
Identificador de organización (organizationIdentifier)	<Identificador legal único de la organización(ej. Número de Registro Único de información fiscal)> **(Requerido)**	
serialNumber (DN)	<Número de identificador único de la persona que usa el certificado> **(Opcional)**	
Departamento (*organizationalUnitName*)	UTF8<La unidad o departamento (útil para perfiles empresariales, ej. “Departamento legal”)> **(Opcional)**	
Dirección de correo (emailAddress)	<La dirección de correo> Es **Opcional** en Subject DN, pero su presencia en la extensión SAN del presente certificado es **Requerido**>	
Localidad(*localityName*)	UTF8<Ciudad o localidad de la organización> **(Opcional)**	
Estado (*stateOrProvinceName*)	UTF8<Información del estado o provincia de la organización> **(Opcional)**	
País (*countryName*)	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)	
NIST CURVE	P-*nnn* donde *nnn* puede ser 256, 384 o 521 **(Requerido)** Aplicar según la curva indicada en la longitud de la firma seleccionada en el “Algoritmo de Firma (*signatureAlgorithm*)”	
*** Para el caso de ECDSA se exigen los campos Anteriores (Requerido)**		
Extensiones		

Restricciones Básicas (basicConstraints) (Opcional)		
Autoridad de Certificación (aC)	Booleano [false]	
Uso de la llave (keyUsage)(Requerido)		
Firma digital	DigitalSignature(0) **(Requerido)**	
Compromiso de contenido (*contentCommitment*)	contentCommitment(1) - <Antes No Repudio - compromiso con el contenido firmado> (Requerido)	
Acuerdo de claves (keyAgreement)	<Para establecer claves de sesión para cifrado del contenido del correo> (Requerido)	
Identificador de clave de Autoridad Certificadora (Authority Key Identifier) (Requerido)		
Clave de Autoridad (*keyIdentifier*)	KeyIdentifier <Identificador de la clave pública de la AC> (Requerido)	
Identificador de la clave del sujeto (Subject Key Identifier) (Recomendable)RFC 5280		
Clave de Autoridad (*keyIdentifier*)	KeyIdentifier <clave pública del propio certificado de la AC>	
Nombre alternativo del sujeto (subjectAlternativeName) (Requerido)		
Formato de correo tradicional	Dirección de correo electrónico <Rfc822Name o SmtpUTF8Mailbox(RFC 9598)> (Requerido)	
Nombre del directorio (directoryname)	<GeneralName> (Opcional)	
Usos Extendidos de la Clave (extKeyUsage) (Requerido)		Definido por el emisor (RFC 5280 y RFC 9336)
Firma de documentos	id-kp-documentSignin 1.3.6.1.4.1.311.10.3.12	
Protección de correo	Id-kp-emailProtection 1.3.6.1.5.5.7.3.4 (Requerido para s/mime)	
Identificador de la clave del sujeto (Subject Key Identifier) (Recomendable)RFC 5280		
Clave de Autoridad (*keyIdentifier*)	KeyIdentifier <clave pública del propio certificado de la AC>	
Puntos de Distribución de las LCR (cRLDistributionPoints) (Requerido)		
Punto de distribución LCR (*distributionPoint*)	<URL HTTP del servicio CRL de la AC>	
AIA (authorityInfoAccess) (Requerido)		
id-ad-ocsp	1.3.6.1.5.5.7.48.1 <URL HTTP del respondedor OCSP de la CA emisora (accessLocation)> (opcional)	
id-ad-caIssuers	1.3.6.1.5.5.7.48.2 <URL HTTP del certificado de la CA emisora (accessLocation)> (opcional, pero debería)	
Políticas de certificado (certificatePolicies)(Requerido)		
PolicyIdentifier (Identificador de política) Requerido		

policy identifier(s)	<Indica la política de la CA que confirma el cumplimiento>	
PolicyQualifiers (Calificador de política)		
cPSuri	<URL de la Declaración de Prácticas de Certificación (DPC/CPS) de la CA emisora>	
Firma		
Algoritmo de Firma (*signatureAlgorithm*)	Algoritmo Autorizado (OID de los algoritmos permitidos mínimo sha256/384/512WithECDSAEncryption)	
Firma (*signature*)	<Contenido de la Firma>	

7.10.7 Estructura de Certificado Electrónico para Profesional Titulado

Certificado cuyo signatario es una persona natural perteneciente a una organización patrocinadora (Gremio o Colegiatura de Profesionales), el cual será destinado para firmar electrónicamente mensajes de datos en función al ejercicio profesional del signatario. Este requisito implica una validación de "Patrocinador validado" ya que el gremio actúa como la entidad que patrocina y valida la relación profesional del suscriptor.

Certificado Profesional Titulado		
Nombre(X.509)	**Tipo de dato [Constante] < Valor >**	**Crítica (para extensiones)**
Datos del Certificado		
Versión (versión)	Entero Hexadecimal[V3] < 0x2 >(Representa la versión 3 del X.509) **(Requerido)**	
Serial (S*erial Number*)	Entero Hexadecimal <Asignado por la AC> (No negativo) **(Requerido)**	
Algoritmo de Firma (*signatureAlgorithm*)	Algoritmo Autorizado (OID de los algoritmo permitido sha256/384/512WithECDSAEncryption)	
Datos de Emisor (issuer)		
Nombre Común (*commonName*)	UTF8 <identificación de la AC principal O Subordinada> **(Requerido)**	
Departamento (*organizationalUnitName*)	UTF8 <División o unidad de la CA (ej. "Departamento de Emisión de Certificados")> **(Opcional)**	
Organización (*organizationName*)	UTF8 [Sistema Nacional de Certificación Electrónica] **(Requerido)**	
Localidad (*localityName*)	UTF8 <Dirección física del Emisor> **(Opcional)**	
Estado (*stateOrProvinceName*)	UTF8 <Estado en el cual se ubica el Emisor> **(Opcional)**	
País (*countryName*)	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*)	<Si la CA elige colocar el nombre completo se debe seguir las directrices de la CA browser Forum BR SMIME>	
Seudónimo(Pseudonym)	<Si **CN** contiene como valor Seudónimo es **Requerido** contener el Alias o sobrenombre verificado y en un atributo aparte, para este caso los atributos Nombre y Apellido no deben estar presentes>	
Nombre (GivenName)	<Nombre del sujeto> (Si el CN es el Nombre Personal completo, es **Requerido** que el certificado use atributos separados, y para este caso Seudónimo no debe estar presente)	
Apellido (Surname)	<Nombre del sujeto> (Si el CN es el Nombre Personal completo, es **Requerido** que el certificado use atributos separados, y para este caso Seudónimo no debe estar presente)	
Nombre de la organización (organizationName)	<Debe contener el nombre legal verificado del patrocinador> **(Requerido)**	
Identificador de la organzación (organizacionIdentifier)	<Debe contener el identificador legal único del patrocinador, ej. Número de registro de información fiscal> **(Requerido)**	
Nombre de la unidad organizativa (organizationalUnitName)	<Unidad o departamento del patrocinador al que pertenece el individuo> **(Opcional)**	
Dirección de correo (emailAdress)	<La dirección de correo> Es O**pcional** en Subject DN, pero su presencia en la extensión SAN del presente certificado es **Requerido**>	
Título (title)	<El título o rol profesional> **(Requerido)**	
Serial (*serialNumber*)	UTF8 <El Número de Colegiado/Matrícula Profesional> **(Opcional)**	
Localidad (*localityName*)	UTF8<Ciudad de ubicación del titular> **(Opcional)**	
Estado (*stateOrProvinceName*)	UTF8 <Estado de ubicación del Titular> **(Opcional)**	
País (*countryName*)	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)	

NIST CURVE	P-*nnn* donde *nnn* puede ser 256, 384 o 521 **(Requerido)** Aplicar según la curva indicada en la longitud de la firma seleccionada en el "Algoritmo de Firma (*signatureAlgorithm*)"	
*** Para el caso de ECDSA se exigen los módulos anteriores**		
Extensiones		
Restricciones Básicas (basicConstraints) (Opcional)		
Autoridad de Certificación(aC)	Booleano [false]	
Uso de la llave (keyUsage) (Requerido)		
Firma digital	digitalSignature(0)	x
Compromiso de contenido (*contentCommitment*)	contentCommitment(1) - <Antes No Repudio - compromiso con el contenido firmado> (Requerido)	
Acuerdo de claves (keyAgreement)	<Para establecer claves de sesión para cifrado del contenido del correo> (**Requerido**)	
Identificador de clave de Autoridad Certificadora (Authority Key Identifier) (Requerido)		
Clave de Autoridad (*keyIdentifier*)	[0]KeyIdentifier <Identificador de la clave pública de la AC emisora> (Requerido)	
Identificador de la clave del sujeto (Subject Key Identifier) (Recomendable)RFC 5280		
Clave de Autoridad (*keyIdentifier*)	KeyIdentifier <clave pública del propio certificado de la AC>	
Nombre alternativo del sujeto (subjectAlternativeName) (Requerido)		
Formato de correo tradicional	Dirección de correo electrónico <Rfc822Name o SmtpUTF8Mailbox(RFC 9598)> (Requerido)	
Nombre del directorio (directoryname)	<GeneralName> (Opcional)	
Usos Extendidos de la Clave (extKeyUsage) (Requerido)		Definido por el emisor (RFC 5280 y RFC 9336)
Firma de documentos	Id-kp-documentSignin 1.3.6.1.4.1.311.10.3.12 (Requerido para firma de documentos)	
Protección de correo	Id-kp-emailProtection 1.3.6.1.5.5.7.3.4 (Requerido para s/mime)	
Puntos de Distribución de las LCR (cRLDistributionPoints) (Requerido)		
Punto de distribución LCR (*distributionPoint*)	<URL HTTP del servicio CRL de la AC>	
AIA (authorityInfoAccess) (Requerido)		
id-ad-ocsp	1.3.6.1.5.5.7.48.1 <URL HTTP del respondedor OCSP de la CA emisora (accessLocation)> (opcional)	

id-ad-caIssuers	1.3.6.1.5.5.7.48.2 <URL HTTP del certificado de la CA emisora (accessLocation)> (opcional, pero debería)	
Políticas de certificado (certificatePolicies)(Requerido)		
PolicyIdentifier (Identificador de política) Requerido		
policy identifier(s)	<Indica la política de la CA que confirma el cumplimiento>	
PolicyQualifiers (Calificador de política)		
cPSuri	<URL de la Declaración de Prácticas de Certificación (DPC/CPS) de la CA emisora>	
Firma		
Algoritmo de Firma (*signatureAlgorithm*)	Algoritmo Autorizado (OID de los algoritmos permitidos mínimo sha256/384/512WithECDSAEncryption)	
Firma (*signature*)	<Contenido de la Firma>	

7.10.8 Estructura de Certificado Electrónico para Empleado de Institución Pública

Certificado cuyo suscriptor es un organismo o ente del Estado Venezolano 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, con relación a la función que desempeña en el cargo. Es del tipo de validación “Perfil validado por patrocinador” porque el organismo o ente del Estado Venezolano actúa como el patrocinador. Esta entidad es la que verifica y garantiza la identidad del funcionario y su relación laboral, y es la que actúa como suscriptor del certificado.

Certificado Empleado de Institución Pública		
Nombre(X.509)	**Tipo de dato [Constante] < Valor >**	**Crítica (para extensiones)**
Datos del Certificado		
Versión (versión)	Entero Hexadecimal [V3] < 0x2 >(Representa la versión 3 del X.509) **(Requerido)**	
Serial (S*erial Number*)	Entero Hexadecimal <Asignado por la AC> (No negativo) **(Requerido)**	
Algoritmo de Firma (*signatureAlgorithm*)	Algoritmo Autorizado (OID de los algoritmo permitido sha256/384/512WithECDSAEncryption)	

Datos de Emisor (*issuer*)		
Nombre Común (*commonName*)	UTF8 <identificación de la AC principal O Subordinada> **(Requerido)**	
Departamento (*organizationalUnitName*)	UTF8 <División o unidad de la CA (ej. "Departamento de Emisión de Certificados"> **(Opcional)**	
Organización (*organizationName*)	UTF8 [Sistema Nacional de Certificación Electrónica] **(Requerido)**	
Localidad(*localityName*)	UTF8 <Dirección física del Emisor> **(Opcional)**	
Estado(*stateOrProvinceName*)	UTF8 <Estado en el cual se ubica el Emisor> **(Opcional)**	
País (*countryName*)	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*)	<Si la CA elige colocar el nombre completo se debe seguir las directrices de la CA browser Forum BR SMIME>	
Seudónimo(Pseudonym)	<Si **CN** contiene como valor Seudónimo es **Requerido** contener el Alias o sobrenombre verificado y en un atributo aparte, para este caso los atributos Nombre y Apellido no deben estar presentes>	
Nombre (GivenName)	<Nombre del sujeto> (Si el CN es el Nombre Personal completo, es **Requerido** que el certificado use atributos separados, y para este caso Seudónimo no debe estar presente)	
Apellido (Surname)	<Nombre del sujeto> (Si el CN es el Nombre Personal completo, es **Requerido** que el certificado use atributos separados, y para este caso Seudónimo no debe estar presente)	
Nombre de la organización (organizationName)	<Nombre Legal del Organismo del Estado (Patrocinador).> **(Requerido)**	
Identificador de la organzación (organizacionIdentifier)	<RIF o Identificador Fiscal del Organismo del Estado.> **(Requerido)**	
Nombre de la unidad organizativa (organizationalUnitName)	<Unidad o departamento del patrocinador al que pertenece el individuo> **(Opcional)**	

Dirección de correo (emailAdress)	<La dirección de correo del funcionario> Es O**pcional** en Subject DN, pero su presencia en la extensión SAN del presente certificado es **Requerido**>	
Titulo (title)	<Cargo que desempeña funcionario> (Opcional)	
Serial (*serialNumber*)	Número de Gaceta/Providencia (o Cédula del Funcionario) (**Opcional**)	
Localidad (*localityName*)	UTF8<Ciudad de ubicación del titular> **(Opcional)**	
Estado (*stateOrProvinceName*)	UTF8 <Estado de ubicación del Titular> **(Opcional)**	
País (*countryName*)	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)	
NIST CURVE	P-*nnn* donde *nnn* puede ser 256, 384 o 521 **(Requerido)** Aplicar según la curva indicada en la longitud de la firma seleccionada en el "Algoritmo de Firma (*signatureAlgorithm*)"	
*** Para el caso de ECDSA se exigen los módulos anteriores**		
Extensiones		
Restricciones Básicas (basicConstraints) (Opcional)		
Autoridad de Certificación(aC)	Booleano [false]	
Uso de la llave (keyUsage) (Requerido)		
Firma digital	digitalSignature(0)	
Compromiso de contenido (*contentCommitment*)	contentCommitment(1) - <Antes No Repudio - compromiso con el contenido firmado> (Requerido)	
Identificador de clave de Autoridad Certificadora (Authority Key Identifier) (Requerido)		
Clave de Autoridad (*keyIdentifier*)	[0]KeyIdentifier <Identificador de la clave pública de la AC emisora> (Requerido)	
Identificador de la clave del sujeto (Subject Key Identifier) (Recomendable)RFC 5280		
Clave de Autoridad (*keyIdentifier*)	KeyIdentifier <clave pública del propio certificado de la AC>	
Nombre alternativo del sujeto (subjectAlternativeName) (Requerido)		
Formato de correo tradicional	Dirección de correo electrónico <Rfc822Name o SmtpUTF8Mailbox(RFC 9598)> (Requerido)	
Nombre del directorio (directoryname)	<GeneralName> (Opcional)	
Usos Extendidos de la Clave (extKeyUsage) (Requerido)		Definido por el emisor (RFC 5280 y RFC 9336)

Firma de documentos	Id-kp-documentSignin 1.3.6.1.4.1.311.10.3.12 (Requerido para firma de documentos)	
Protección de correo	Id-kp-emailProtection 1.3.6.1.5.5.7.3.4 (Requerido para s/mime)	
Puntos de Distribución de las LCR (cRLDistributionPoints) (Requerido)		
Punto de distribución LCR (*distributionPoint*)	<URL HTTP del servicio CRL de la AC>	
AIA (authorityInfoAccess) (Requerido)		
id-ad-ocsp	1.3.6.1.5.5.7.48.1 <URL HTTP del respondedor OCSP de la CA emisora (accessLocation)> (opcional)	
id-ad-caIssuers	1.3.6.1.5.5.7.48.2 <URL HTTP del certificado de la CA emisora (accessLocation)> (opcional, pero debería)	
Políticas de certificado (certificatePolicies)(Requerido)		
PolicyIdentifier (Identificador de política) Requerido		
policy identifier(s)	<Indica la política de la CA que confirma el cumplimiento>	
PolicyQualifiers (Calificador de política)		
cPSuri	<URL de la Declaración de Prácticas de Certificación (DPC/CPS) de la CA emisora>	
Firma		
Algoritmo de Firma (*signatureAlgorithm*)	Algoritmo Autorizado (OID de los algoritmos permitidos mínimo sha256/384/512WithECDSAEncryption)	
Firma(*signature*)	<Contenido de la Firma>	

7.10.9 Estructura de Certificado Electrónico para Empleado de Empresa Privada

Certificado que identifica a una persona natural como empleado de una empresa privada, se destina para firmar electrónicamente mensajes de datos, con relación a la función que desempeña en la empresa. Es del tipo de validación “Perfil validado por patrocinador” porque la institución actúa como el patrocinador que verifica la identidad de la persona y su relación laboral.

Certificado de Empleado de Empresa Privada		
Nombre(X.509)	**Tipo de dato [Constante] < Valor >**	**Crítica (para extensiones)**
Datos del Certificado		

Versión (*versión*)	Entero Hexadecimal [V3] < 0x2 >(Representa la versión 3 del X.509) **(Requerido)**	
Serial (S*erial Number*)	Entero Hexadecimal <Asignado por la AC> (No negativo) **(Requerido)**	
Algoritmo de Firma (*signatureAlgorithm*)	Algoritmo Autorizado (OID de los algoritmo permitido sha256/384/512WithECDSAEncryption)	
Datos de Emisor (issuer)		
Nombre Común (*commonName*)	UTF8 <identificación de la AC principal O Subordinada> **(Requerido)**	
Organización (*organizationName*)	UTF8 [Sistema Nacional de Certificación Electrónica] **(Requerido)**	
Departamento (*organizationalUnitName*)	UTF8 <División o unidad de la CA (ej. "Departamento de Emisión de Certificados")> **(Opcional)**	
Localidad(*localityName*)	UTF8 <Ciudad de ubicación del Emisor> **(Opcional)**	
Estado (*stateOrProvinceName*)	UTF8 <Estado en el cual se ubica el Emisor> **(Opcional)**	
País (*countryName*)	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*)	<Si la CA elige colocar el nombre completo se debe seguir las directrices de la CA browser Forum BR SMIME>	
Seudónimo(Pseudonym)	<Si contiene este campo es **Requerido** contener el Alias o sobrenombre verificado, los atributos Nombre y Apellido no deben estar presentes>	
Nombre (GivenName)	<Nombre del sujeto> (Si el CN es el Nombre Personal es **Requerido** que el certificado use atributos separados, y para este caso Seudónimo no debe estar presente)	
Apellido (Surname)	<Nombre del sujeto> (Si el CN es el Nombre Personal es **Requerido** que el certificado use atributos separados, y para este caso Seudónimo no debe estar presente)	
Nombre de la organización (organizationName)	<Debe contener el nombre legal verificado del patrocinador> **(Requerido)**	
Identificador de la organzación (organizacionIdentifier)	<Debe contener el identificador legal único del patrocinador, ej. Número de registro de información fiscal> **(Requerido)**	

Nombre de la unidad organizativa (organizationalUnitName)	<Unidad o departamento del patrocinador al que pertenece el individuo> **(Opcional)**	
Dirección de correo (emailAdress)	<La dirección de correo> Es O**pcional** en Subject DN, pero su presencia en la extensión SAN del presente certificado es **Requerido**>	
Titulo (title)	<Cargo que desempeña el titular del certificado> (Opcional)	
Serial (*serialNumber*)	Identificación fiscal o legal de la entidad **(Opcional)**	
Localidad (*localityName*)	UTF8<Ciudad de ubicación del titular> **(Opcional)**	
Estado (*stateOrProvinceName*)	UTF8 <Estado de ubicación del Titular> **(Opcional)**	
País (*countryName*)	UTF8 [VE] (ISO 3166-1-alpha-2) **(Requerido)**	
Información de Clave Pública del Titular (*subjectPublicKey*)		
Algoritmo de clave pública (*algorithm*)	<AlgoritmoAsignado>(ecdsaEncryption, dhpublicnumber,id-ecdsa, id-ecdsaPublicKey)	
NIST CURVE	P-*nnn* donde *nnn* puede ser 256, 384 o 521 **(Requerido)** Aplicar según la curva indicada en la longitud de la firma seleccionada en el "Algoritmo de Firma (*signatureAlgorithm*)"	
*** Para el caso de ECDSA se exigen en los módulos anteriores**		
Extensiones		
Restricciones Básicas (basicConstraints) (Opcional)		
Autoridad de Certificación(aC)	Booleano [false]	
Uso de la llave (keyUsage) (Requerido)		x
Firma digital	DigitalSignature(0) (**Requerido)**	
Compromiso de contenido (*contentCommitment*)	contentCommitment(1) - <Antes No Repudio - compromiso con el contenido firmado> (Requerido)	
Acuerdo de claves (keyAgreement)	<Para establecer claves de sesión para cifrado del contenido del correo> (Requerido)	
Identificador de clave de Autoridad Certificadora (Authority Key Identifier) (Requerido)		
Clave de Autoridad (*keyIdentifier*)	KeyIdentifier <Identificador de la clave pública de la AC> (Requerido)	
Identificador de la clave del sujeto (Subject Key Identifier) (Recomendable)RFC 5280		
Clave de Autoridad (*keyIdentifier*)	KeyIdentifier <clave pública del propio certificado de la AC>	
Nombre alternativo del sujeto (subjectAlternativeName) (Requerido)		
Formato de correo tradicional	Dirección de correo electrónico <Rfc822Name o SmtpUTF8Mailbox(RFC 9598)> (Requerido)	

Nombre del directorio (directoryname)	<GeneralName> (Opcional)	
Usos Extendidos de la Clave (extKeyUsage) (Requerido)		Definido por el emisor (RFC 5280 y RFC 9336)
Firma de documentos	Id-kp-documentSignin 1.3.6.1.4.1.311.10.3.12 (Requerido para firma de documentos)	
Protección de correo	Id-kp-emailProtection 1.3.6.1.5.5.7.3.4 (Requerido para s/mime)	
Puntos de Distribución de las LCR (cRLDistributionPoints) (Requerido)		
Punto de distribución LCR (*distributionPoint*)	<URL HTTP del servicio CRL de la AC>	
AIA (*authorityInfoAccess*) (Requerido)		
id-ad-ocsp	1.3.6.1.5.5.7.48.1 <URL HTTP del respondedor OCSP de la CA emisora (accessLocation)> (opcional)	
id-ad-caIssuers	1.3.6.1.5.5.7.48.2 <URL HTTP del certificado de la CA emisora (accessLocation)> (opcional, pero debería)	
Políticas de certificado (certificatePolicies)(Requerido)		
PolicyIdentifier (Identificador de política) Requerido		
policy identifier(s)	<Indica la política de la CA que confirma el cumplimiento>	
PolicyQualifiers (Calificador de política)		
cPSuri	<URL de la Declaración de Prácticas de Certificación (DPC/CPS) de la CA emisora>	
Firma		
Algoritmo de Firma (*signatureAlgorithm*)	Algoritmo Autorizado (OID de los algoritmo permitido sha256/384/512WithECDSAEncryption)	
Firma(*signature*)	<Contenido de la Firma>	

7.10.10 Estructura de Certificado Electrónico para la Cédula Electrónica

Certificado cuyo titular es una persona natural, teniendo como finalidad su identificación. Este sólo podrá ser emitido por las autoridades de certificación del ente con competencia en identificación (ej. SAIME). Posee atributos especiales para describir detalles del titular. Manteniendo un doble propósito especifico como Identificación Individual (IV) y Autenticación de cliente (ClientAuth) probando criptográficamente su identidad.

Certificado para la Cédula Electrónica		
Nombre(X.509)	**Tipo de dato [Constante] < Valor >**	**Crítica (para extensiones)**
Datos del Certificado		

Versión (versión)	Entero Hexadecimal [V3] < 0x2 >(Representa la versión 3 del X.509) **(Requerido)**	
Serial (S*erial Number*)	Entero Hexadecimal <Asignado por la AC> (No negativo) **(Requerido)**	
Algoritmo de Firma (*signatureAlgorithm*)	Algoritmo Autorizado (OID de los algoritmo permitido sha256/384/512WithECDSAEncryption)	
Datos de Emisor (*issuer*)		
Nombre Común (*commonName*)	UTF8 <identificación de la AC principal O Subordinada> **(Requerido)**	
Departamento (*organizationalUnitName*)	UTF8 <División o unidad de la CA (ej. "Departamento de Emisión de Certificados")> **(Opcional)**	
Organización (*organizationName*)	UTF8 [Sistema Nacional de Certificación Electrónica] **(Requerido)**	
Localidad(*localityName*)	UTF8 <Dirección física del Emisor> **(Opcional)**	
Estado (*stateOrProvinceName*)	UTF8 <Estado en el cual se ubica el Emisor> **(Opcional)**	
País (*countryName*)	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<El nombre completo del titular> **(Requerido)**	
serialNumber (DN)	<Identificación fiscal o legal de la entidad> **(Requerido)**	
País(*countryName*)	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)	
NIST CURVE	P-*nnn* donde *nnn* puede ser 256, 384 o 521 **(Requerido)** Aplicar según la curva indicada en la longitud de la firma seleccionada en el "Algoritmo de Firma (*signatureAlgorithm*)"	
Extensiones		
Atributos Adicionales del Titular (*subjectDirectoryAttributes*) (Opcional)RFC 5280		
Fecha de Nacimiento (*dateOfBirth*)	<Fecha de Nacimiento del Titular> **(Opcional)**	
Lugar de Nacimiento (*placeOfBirth*)	<Lugar de Nacimiento del Titular> **(Opcional)**	

Género (*gender*)	<El género legal del titular>() **(Opcional)**	
Nacionalidad(countryOfCitizenship)	<Indica la ciudadanía del titular, importante en un documento de identidad.> **(Opcional)**	
Domicilio/Dirección (postalAddress)	<La dirección de residencia registrada.> (Opcional)	
Restricciones Básicas (basicConstraints) (Opcional)		
Autoridad de Certificación(aC)	Booleano [false]	
Uso de la llave (*keyUsage*) (Requerido)		
Firma digital	digitalSignature(0)	
Compromiso de contenido (*contentCommitment*)	contentCommitment(1) - (Antes No Repudio - compromiso con el contenido firmado)	
Información Biométrica (biometricInfo) (Opcional) RFC3739		
Tipos de datos biométricos (*typeOfBiometricData*)	<Tipo de información biométrica que hace 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>	
Identificador de clave de Autoridad Certificadora (Authority Key Identifier) (Requerido)		
Clave de Autoridad (*keyIdentifier*)	KeyIdentifier <Identificador de la clave pública de la AC> (Requerido)	
Identificador de la clave del sujeto (Subject Key Identifier) (Recomendable)RFC 5280		
Clave de Autoridad (*keyIdentifier*)	KeyIdentifier <clave pública del propio certificado de la AC>	
Usos Extendidos de la Clave (extKeyUsage) (Opcional)		
Firma de documentos	id-kp-documentSignin 1.3.6.1.4.1.311.10.3.12	
Autenticación de cliente	ClientAuth 1.3.6.1.5.5.7.3.2 (Requerido)	
Puntos de Distribución de las LCR (cRLDistributionPoints) (Requerido)		
Punto de distribución LCR (*distributionPoint*)	<URL HTTP del servicio CRL de la AC>	
AIA (authorityInfoAccess) (Requerido)		
id-ad-ocsp	1.3.6.1.5.5.7.48.1 <URL HTTP del respondedor OCSP de la CA emisora (accessLocation)> (opcional)	
id-ad-caIssuers	1.3.6.1.5.5.7.48.2 <URL HTTP del certificado de la CA emisora (accessLocation)> (opcional, pero debería)	
Políticas de certificado (certificatePolicies)(Requerido)		
PolicyIdentifier (Identificador de política) Requerido		

policy identifier(s)	<Indica la política de la CA que confirma el cumplimiento>	
PolicyQualifiers (Calificador de política)		
cPSuri	<URL de la Declaración de Prácticas de Certificación (DPC/CPS) de la CA emisora>	
Firma		
Algoritmo de Firma (*signatureAlgorithm*)	Algoritmo Autorizado (OID de los algoritmo permitido sha256/384/512WithECDSAEncryption)	
Firma(*signature*)	<Contenido de la Firma>	

7.10.11 Estructura de Certificado Electrónico para Servidor

Certificado cuyo suscriptor es una persona jurídica, siendo su principal objetivo 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 de Conexiones VPN, Servidor de Correo Electrónico, entre otras, también se pueden hacer implementaciones más específicas agregando Claves de Usos y Claves Usos Extendidos. Su clasificación se refuerza como SSL/TLS con dos niveles de validación como Organización validada (OV) y Validación extendida (EV). Si requiere un control distinto de validación seguir las directrices de la CA Browser Forum TLS BR.

Certificado de Servidor (General)		
Nombre(X.509)	**Tipo de dato [Constante] < Valor > (Observaciones)**	**Crítica (para extensiones)**
Datos del Certificado		
Versión (*versión*)	Entero Hexadecimal [V3] < 0x2 >(Representa la versión 3 del X.509)	
Serial (Serial Number)	Entero Hexadecimal <Asignado por la AC> (No negativo)	
Algoritmo de Firma (*signatureAlgorithm*)	Algoritmo Autorizado (OID de los algoritmo permitido sha256/384/512WithECDSAEncryption)	
Datos de Emisor (*issuer*)		
Nombre Común (*commonName*)	UTF8 <identificación de la AC principal O Subordinada> **(Requerido)**	

Departamento (*organizationalUnitName*)	UTF8 <División o unidad de la CA (ej. "Departamento de Emisión de Certificados")> **(Opcional)**	
Organización (*organizationName*)	UTF8 [Sistema Nacional de Certificación Electrónica] **(Requerido)**	
Localidad (*localityName*)	UTF8 <Dirección física del Emisor> **(Opcional)**	
Estado (*stateOrProvinceName*)	UTF8 <Estado en el cual se ubica el Emisor> **(Opcional)**	
País (*countryName*)	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*)		
Componente de dominio (domainComponent)	<Si esta presente requiere una etiqueta de dominio válida> **(Opcional y solo aplica para OV)**	
Organización (*organizationName*)	UTF8 <Nombre del titular y/o comercial) **(Requerido para ambas validaciones)**	
Categoría de negocio(businessCategory)	<Debe contener por lo menos una de las siguientes: Organización privada, entidad gubernamental, Entidad comercial o Entidad sin fines de lucro >**(Requerido para EV)**	
Estado (stateOrProvinceName)	UTF8 <El nombre del titular y/o nombre comercial.> **[Opcional para OV. Si falta el campo (`localityName`) es requerido Organización] (Necesario para EV)**	
Localidad(*localityName*)	UTF8<Localidad del titular> **(Opcional para OV, necesario para EV)**	
Número de serie (seriaLNumber)	<Debe contener el número de registro (o similar) del sujeto> **(Requerido solo para EV) Browser-Forum-EV-Guidelines**	
País (*countryName*)	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)	
NIST CURVE	P-*nnn* donde *nnn* puede ser 256, 384 o 521 **(Requerido)** Aplicar según la curva indicada en la longitud de la firma seleccionada en el "Algoritmo de Firma (*signatureAlgorithm*)"	

*** Para el caso de ECDSA se exigen los módulos anteriores**		
Extensiones		
Restricciones Básicas (basicConstraints) (Opcional)		
Autoridad de Certificación(aC)	Booleano [false]	
Uso de la llave (keyUsage) (Requerido)		
Firma digital	digitalSignature(0)	
Nombre Alternativo del Titular (subjectAltName) (Requerido)		
Nombres de Dominio (dNSName)	<Sitio Web de la Empresa> (NO puede contener "Internal Names" (nombres reservados/internalos)	
Dirección IP válida (iPAddress)	<La entrada NO DEBE contener Una dirección IP reservada.>	
Usos Extendidos de la Clave (extKeyUsage) (Requerido)		
Autenticación de Servidor	serverAuth 1.3.6.1.5.5.7.3.1 (Requerido)	
Autenticación de Cliente	clientAuth 1.3.6.1.5.5.7.3.2 (opcional)	
Puntos de Distribución de las LCR (cRLDistributionPoints) (Requerido)		
Punto de distribución LCR (*distributionPoint)*	<URL HTTP del servicio CRL de la AC>	
AIA (authorityInfoAccess) (Requerido)		
id-ad-ocsp	1.3.6.1.5.5.7.48.1 <URL HTTP del respondedor OCSP de la CA emisora (accessLocation)> (opcional)	
id-ad-caIssuers	1.3.6.1.5.5.7.48.2 <URL HTTP del certificado de la CA emisora (accessLocation)> (opcional, pero debería)	
Identificador de clave de Autoridad Certificadora (Authority Key Identifier) (Requerido)		
Clave de Autoridad (keyIdentifier)	[0]KeyIdentifier <Identificador de la clave pública de la AC> (Requerido)	
Políticas de certificado (certificatePolicies)(Requerido)		
PolicyIdentifier (Identificador de política) Requerido		
policy identifier(s)	<Indica la política de la CA que confirma el cumplimiento>	
PolicyQualifiers (Calificador de política)		
cPSuri	<URL de la Declaración de Prácticas de Certificación (DPC/CPS) de la CA emisora>	
Firma		
Algoritmo de Firma (*signatureAlgorithm*)	Algoritmo Autorizado (OID de los algoritmos permitidos mínimo sha256/384/512WithECDSAEncryption)	
Firma(signature)	<Contenido de la Firma>	

7.10.12 Estructura de Certificado Electrónico para Dispositivos Móviles

Certificado cuyo suscriptor es una persona jurídica o natural, que identifica y verifica un dispositivo móvil, permitiendo que la comunicación de este ante la red sea efectiva. Su función principal es probar la identidad del dispositivo ante una red o servidor para establecer una conexión segura y de confianza. Perteneciente a la Validación Individual (IV) se valida la identidad personal del usuario asociado al dispositivo y a la Organización validada (OV) se valida la existencia legal de la empresa propietaria del dispositivo. Si requiere un control mas estricto de acceso y propiedad puede optar por Validación Extendida (EV) siguiendo las directrices de la CA Browser Forum TLS BR.

Certificado de Dispositivos Móviles		
Nombre(X.509)	**Tipo de dato [Constante] < Valor > (Observaciones)**	**Crítica (para extensiones)**
Datos del Certificado		
Versión (versión)	Entero Hexadecimal [V3] < 0x2 >(Representa la versión 3 del X.509) **(Requerido)**	
Serial (*serialNumber*)	Entero Hexadecimal <Asignado por la AC> (No negativo) **(Requerido)**	
Algoritmo de Firma (*signatureAlgorithm*)	Algoritmo Autorizado (OID de los algoritmo permitido sha256/384/512WithECDSAEncryption)	
Datos de Emisor (issuer)		
Nombre Común (*commonName*)	UTF8 <identificación de la AC principal O Subordinada> **(Requerido)**	
Departamento (*organizationalUnitName*)	UTF8 <División o unidad de la CA (ej. "Departamento de Emisión de Certificados")> **(Opcional)**	
Organización (*organizationName*)	UTF8 [Sistema Nacional de Certificación Electrónica] **(Requerido)**	
Localidad(*localityName*)	UTF8 <Dirección física del Emisor> **(Opcional)**	
Estado (*stateOrProvinceName*)	UTF8 <Estado en el cual se ubica el Emisor> **(Opcional)**	
País (*countryName*)	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)		
Componente de dominio (domainComponent)	<Si esta presente requiere una etiqueta de dominio válida> **(Opcional y solo aplica para OV)**	

Apellido (surname)	<Apellido del titular> **(Requerido para IV, no aplica para OV)**	
Nombre de pila (givenName)	<Nombre del titular> (**Requerido para IV, no aplica para OV)**	
Organización (*organizationName*)	**UTF8 <**Nombre del titular y/o comercial>**(Requerido)**	
Localidad(*localityName*)	UTF8<Localidad del titular> **(Opcional)**	
Estado (*stateOrProvinceName*)	UTF8UTF8 <El nombre del titular y/o nombre comercial.> **[No recomendado para IV y Opcional para OV (Si falta el campo `localityName` es requerido Organización]**>	
País (*countryName*)	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)	
NIST CURVE	P-*nnn* donde *nnn* puede ser 256, 384 o 521 **(Requerido)** Aplicar según la curva indicada en la longitud de la firma seleccionada en el "Algoritmo de Firma (*signatureAlgorithm*)"	
*** Para el caso de ECDSA se exigen los módulos anteriores**		
Extensiones		
Restricciones Básicas (basicConstraints) (Opcional)		
Autoridad de Certificación(aC)	Booleano [false]	
Uso de la llave (keyUsage) (Requerido)		
Firma digital	digitalSignature(0)	
Identificador de clave de Autoridad Certificadora (Authority Key Identifier) (Opcional)		
Clave de Autoridad(*keyIdentifier*)	KeyIdentifier <Identificador de la clave pública de la AC>	
Nombre Alternativo del Titular (subjectAltName) (Requerido)		
Nombres de Dominio (dNSName)	<Sitio Web de la Empresa> (NO puede contener "Internal Names" (nombres reservados/internalos)	
Dirección IP válida (iPAddress)	<La entrada NO DEBE contener Una dirección IP reservada.>	
Usos Extendidos de la Clave (extKeyUsage) (Requerido)		
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	
Puntos de Distribución de las LCR (cRLDistributionPoints) (Requerido)		

Punto de distribución LCR (*distributionPoint*)	<URL HTTP del servicio CRL de la AC>	
AIA (authorityInfoAccess) (Requerido)		
id-ad-ocsp	1.3.6.1.5.5.7.48.1 <URL HTTP del respondedor OCSP de la CA emisora (accessLocation)> (opcional)	
id-ad-calssuers	1.3.6.1.5.5.7.48.2 <URL HTTP del certificado de la CA emisora (accessLocation)> (opcional, pero debería)	
Políticas de certificado (certificatePolicies)(Requerido)		
PolicyIdentifier (Identificador de política) Requerido		
policy identifier(s)	<Indica la política de la CA que confirma el cumplimiento>	
PolicyQualifiers (Calificador de política)		
cPSuri	<URL de la Declaración de Prácticas de Certificación (DPC/CPS) de la CA emisora>	
Firma		
Algoritmo de Firma (*signatureAlgoritm*)	Algoritmo Autorizado (OID de los algoritmo permitido sha256/384/512WithECDSAEncryption).	
Firma(*signature*)	<Contenido de la Firma>	

7.10.13 Estructura de Certificado Electrónico para Banca Electrónica

Certificado cuyo suscriptor es una persona jurídica, se utiliza para autenticar al titular ante el servidor bancario, así como para la firma de ordenes de pago (transacciones electrónicas) realizadas en la misma. La siguiente estructura va enfocado en la validación de “Perfil validado por patrocinador” porque la persona jurídica actúa como el patrocinador que verifica la identidad del empleado y autoriza a firmar y autenticarse ante el banco. En el caso del tipo “Perfil validado por organización” (OV) se debe seguir las directrices de la CA browser Forum SMIMEBR para el uso de esta validación.

Banca Electrónica		
Nombre(X.509)	**Tipo de dato [Constante] < Valor >**	**Crítica (para extensiones)**
Datos del Certificado		
Versión (versión)	Entero Hexadecimal [V3] < 0x2 >(Representa la versión 3 del X.509)	
Serial (*Serial Number*)	Entero Hexadecimal <Asignado por la AC> **(No negativo)**	
Algoritmo de Firma (*signatureAlgorithm*)	Algoritmo Autorizado (OID de los algoritmos permitidos mínimo sha256/384/512WithECDSAEncryption)	

Datos de Emisor (issuer)		
Nombre Común (*commonName*)	UTF8 <identificación de la AC principal O Subordinada> **(Requerido)**	
Departamento (*organizationalUnitName*)	UTF8 <División o unidad de la CA (ej. "Departamento de Emisión de Certificados")> **(Opcional)**	
Organización (*organizationName*)	UTF8 [Sistema Nacional de Certificación Electrónica] **(Requerido)**	
Localidad(*localityName*)	UTF8 <Dirección física del Emisor> **(Opcional)**	
Estado (*stateOrProvinceName*)	UTF8 <Estado en el cual se ubica el Emisor> **(Opcional)**	
País (*countryName*)	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*)	<Si la CA elige colocar el nombre completo se debe seguir las directrices de la CA browser Forum BR SMIME>	
Seudónimo(Pseudonym)	<Si contiene este campo es **Requerido** contener el Alias o sobrenombre verificado, los atributos Nombre y Apellido no deben estar presentes>	
Nombre (GivenName)	<Nombre del sujeto> (Si el CN es el Nombre Personal es **Requerido** que el certificado use atributos separados, y para este caso Seudónimo no debe estar presente)	
Apellido (Surname)	<Nombre del sujeto> (Si el CN es el Nombre Personal es **Requerido** que el certificado use atributos separados, y para este caso Seudónimo no debe estar presente)	
Nombre de la organización (organizationName)	<Debe contener el nombre legal verificado del patrocinador> **(Requerido)**	
Identificador de la organzación (organizacionIdentifier)	<Debe contener el identificador legal único del patrocinador, ej. Número de registro de información fiscal> **(Requerido)**	
Nombre de la unidad organizativa (organizationalUnitName)	<Unidad o departamento del patrocinador al que pertenece el individuo> **(Opcional)**	
Dirección de correo (emailAdress)	<La dirección de correo> Es **Opcional** en Subject DN, pero su presencia en la extensión SAN del presente certificado es **Requerido**>	
Titulo (title)	<Cargo que desempeña el titular del certificado> (Opcional)	
Serial (*serialNumber*)	Identificación fiscal o legal de la entidad **(Opcional)**	
Localidad (*localityName*)	UTF8<Ciudad de ubicación del titular> **(Opcional)**	
Estado (*stateOrProvinceName*)	UTF8 <Estado de ubicación del Titular> **(Opcional)**	

País (*countryName*)	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)	
NIST CURVE	P-*nnn* donde *nnn* puede ser 256, 384 o 521 **(Requerido)** Aplicar según la curva indicada en la longitud de la firma seleccionada en el "Algoritmo de Firma (*signatureAlgorithm*)"	
*** Para el caso de ECDSA se exigen los módulos anteriores**		
Extensiones		
Restricciones Básicas (basicConstraints) (Opcional)		
Autoridad de Certificación(aC)	Booleano [false]	
Uso de la llave (keyUsage) (Requerido)		x
Firma digital	DigitalSignature(0) (Requerido)	
Compromiso de contenido (*contentCommitment*)	contentCommitment(1) - (Antes No Repudio - - compromiso con el contenido firmado> **Puede ser usada (SMIMEBR)**	
Acuerdo de claves (keyAgreement)	<Para establecer claves de sesión para cifrado del contenido del correo> (Requerido)	
Identificador de clave de Autoridad Certificadora (Authority Key Identifier) (Requerido)		
Clave de Autoridad (*keyIdentifier*)	[0]KeyIdentifier <Identificador de la clave pública de la AC emisora> (Requerido)	
Identificador de la clave del sujeto (Subject Key Identifier) (Recomendable)RFC 5280		
Clave de Autoridad (*keyIdentifier*)	KeyIdentifier <clave pública del propio certificado de la AC>	
Nombre alternativo del sujeto (subjectAlternativeName) (Requerido)		
Formato de correo tradicional	Dirección de correo electrónico <Rfc822Name o SmtpUTF8Mailbox(RFC 9598)> (Requerido)	
Nombre del directorio (directoryname)	<GeneralName> (Opcional)	
Usos Extendidos de la Clave (extKeyUsage) (Requerido)		Definido por el emisor (RFC 5280 y RFC 9336)
Firma de documentos	Id-kp-documentSignin 1.3.6.1.4.1.311.10.3.12 (Requerido para firma de documentos)	
Protección de correo	Id-kp-emailProtection 1.3.6.1.5.5.7.3.4 (Requerido para s/mime)	
Puntos de Distribución de las LCR (cRLDistributionPoints) (Requerido)		
Punto de distribución LCR (*distributionPoint*)	<URL HTTP del servicio CRL de la AC>	

AIA (authorityInfoAccess) (Requerido)		
id-ad-ocsp	1.3.6.1.5.5.7.48.1 <URL HTTP del respondedor OCSP de la CA emisora (accessLocation)> (opcional)	
id-ad-calssuers	1.3.6.1.5.5.7.48.2 <URL HTTP del certificado de la CA emisora (accessLocation)> (opcional, pero debería)	
Políticas de certificado (certificatePolicies)(Requerido)		
PolicyIdentifier (Identificador de política) Requerido		
policy identifier(s)	<Indica la política de la CA que confirma el cumplimiento>	
PolicyQualifiers (Calificador de política)		
cPSuri	<URL de la Declaración de Prácticas de Certificación (DPC/CPS) de la CA emisora>	
Firma		
Algoritmo de Firma (*signatureAlgorithm*)	Algoritmo Autorizado (OID de los algoritmo permitido sha256/384/512WithECDSAEncryption)	
Firma(*signature*)	<Contenido de la Firma>	

7.10.14 Estructura de Certificado Electrónico para Representante de Institución Pública

Certificado que identifica a una persona natural como representante legal de una institución pública, permitiéndole suscribir documentos a nombre del organismo. Es del tipo de validación “Perfil validado por patrocinador” porque la institución actúa como el patrocinador que verifica la identidad de la persona y su relación laboral. La identidad legal (patrocinador) autoriza al individuo actuar por ella.

Representante de Empresa Pública		
Nombre(X.509)	**Tipo de dato [Constante] < Valor >**	**Crítica (para extensiones)**
Datos del Certificado		
Versión (versión)	Entero Hexadecimal [V3] < 0x2 >(Representa la versión 3 del X.509)	
Serial (*Serial Number*)	Entero Hexadecimal <Asignado por la AC> (No negativo)	
Algoritmo de Firma (*signatureAlgorithm*)	Algoritmo Autorizado (OID de los algoritmo permitido sha256/384/512WithECDSAEncryption)	
Datos de Emisor (*issuer*)		
Nombre Común (*commonName*)	UTF8 <identificación de la AC principal O Subordinada> **(Requerido)**	
Departamento (*organizationalUnitName*)	UTF8 <División o unidad de la CA (ej. "Departamento de Emisión de Certificados")> **(Opcional)**	

Organización (*organizationName*)	UTF8 [Sistema Nacional de Certificación Electrónica] **(Requerido)**	
Localidad(*localityName*)	UTF8 <Dirección física del Emisor> **(Opcional)**	
Estado(*stateOrProvinceName*)	UTF8 <Estado en el cual se ubica el Emisor> **(Opcional)**	
País (*countryName*)	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*)	<Si la CA elige colocar el nombre completo se debe seguir las directrices de la CA browser Forum BR SMIME>	
Seudónimo(Pseudonym)	<Si contiene este campo es **Requerido** contener el Alias o sobrenombre verificado, los atributos Nombre y Apellido no deben estar presentes>	
Nombre (GivenName)	<Nombre del sujeto> (Si el CN es el Nombre Personal es **Requerido** que el certificado use atributos separados, y para este caso Seudónimo no debe estar presente)	
Apellido (Surname)	<Nombre del sujeto> (Si el CN es el Nombre Personal es **Requerido** que el certificado use atributos separados, y para este caso Seudónimo no debe estar presente)	
Nombre de la organización (organizationName)	<Debe contener el nombre legal verificado del patrocinador> **(Requerido)**	
Identificador de la organzación (organizacionIdentifier)	<Debe contener el identificador legal único del patrocinador, ej. Número de registro de información fiscal> **(Requerido)**	
Nombre de la unidad organizativa (organizationalUnitName)	<Unidad o departamento del patrocinador al que pertenece el individuo> **(Opcional)**	
Dirección de correo (emailAdress)	<La dirección de correo> Es O**pcional** en Subject DN, pero su presencia en la extensión SAN del presente certificado es **Requerido**>	
Titulo (title)	<Cargo que desempeña el titular del certificado> (Opcional)	
Serial (*serialNumber*)	Identificación fiscal o legal de la entidad **(Opcional)**	
Localidad (*localityName*)	UTF8<Ciudad de ubicación del titular> **(Opcional)**	
Estado (*stateOrProvinceName*)	UTF8 <Estado de ubicación del Titular> **(Opcional)**	
País (*countryName*)	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)	
NIST CURVE	P-*nnn* donde *nnn* puede ser 256, 384 o 521 **(Requerido)** Aplicar según la curva indicada en la longitud de la firma seleccionada en el "Algoritmo de Firma (*signatureAlgorithm*)"	
*** Para el caso de ECDSA se exigen los módulos anteriores**		
Extensiones		
Restricciones Básicas (basicConstraints) (Opcional)		
Autoridad de Certificación(aC)	Booleano [false]	
Uso de la llave (keyUsage) (Requerido)		
Firma digital	DigitalSignature(0) (**Requerido)**	
Compromiso de contenido (*contentCommitment*)	contentCommitment(1) - <Antes No Repudio - compromiso con el contenido firmado> (Requerido)	
Acuerdo de claves (keyAgreement)	<Para establecer claves de sesión para cifrado del contenido del correo> (Requerido)	
Identificador de clave de Autoridad Certificadora (Authority Key Identifier) (Requerido)		
Clave de Autoridad (*keyIdentifier*)	[0]KeyIdentifier <Identificador de la clave pública de la AC emisora> (Requerido)	
Identificador de la clave del sujeto (Subject Key Identifier) (Recomendable) RFC 5280		
Clave de Autoridad (*keyIdentifier*)	KeyIdentifier <clave pública del propio certificado de la AC>	
Nombre alternativo del sujeto (subjectAlternativeName) (Requerido)		
Formato de correo tradicional	Dirección de correo electrónico <Rfc822Name o SmtpUTF8Mailbox(RFC 9598)> (Requerido)	
Nombre del directorio (directoryname)	<GeneralName> (Opcional)	
Usos Extendidos de la Clave (extKeyUsage) (Requerido)		Definido por el emisor (RFC 5280 y RFC 9336)
Firma de documentos	Id-kp-documentSignin 1.3.6.1.4.1.311.10.3.12 (Requerido para firma de documentos)	
Protección de correo	Id-kp-emailProtection 1.3.6.1.5.5.7.3.4 (Requerido para s/mime)	
Puntos de Distribución de las LCR (cRLDistributionPoints) (Requerido)		
Punto de distribución LCR (*distributionPoint*)	<URL HTTP del servicio CRL de la AC>	
AIA (authorityInfoAccess) (Requerido)		

id-ad-ocsp	1.3.6.1.5.5.7.48.1 <URL HTTP del respondedor OCSP de la CA emisora (accessLocation)> (opcional)	
id-ad-calssuers	1.3.6.1.5.5.7.48.2 <URL HTTP del certificado de la CA emisora (accessLocation)> (opcional, pero debería)	
Políticas de certificado (certificatePolicies)(Requerido)		
PolicyIdentifier (PC/CP) (Requerido)		
policyIdentifier(s)	<Indica la política de la CA que confirma el cumplimiento>	
PolicyQualifiers (DPC/CPS) (Opcional)		
cPSuri	<URL de la Declaración de Prácticas de Certificación (CPS) de la CA emisora>	
Firma		
Algoritmo de Firma (*signatureAlgorithm*)	Algoritmo Autorizado (OID de los algoritmo permitido sha256/384/512WithECDSAEncryption)	
Firma(*signature*)	<Contenido de la Firma>	

7.10.15 Estructura de Certificado Electrónico para Representante de Empresa Privada

Certificado que identifica a una persona natural como representante legal de una empresa privada, permitiéndole suscribir documentos a nombre de la organización. Se pueden obtener diversas aplicaciones utilizando combinación de Claves de Usos y Claves de Usos Extendidos. Es del tipo de validación “Perfil validado por patrocinador” porque el certificado identifica a la persona natural (representante) y a la empresa privada (patrocinador) otorgando la autoridad al individuo para actuar en su nombre. Si requiere otro tipo de validación seguir las directrices de la **CA Browser Forum SMIMEBR.**

Representante de Empresa Privada		
Nombre(X.509)	**Tipo de dato [Constante] < Valor >**	**Crítica (para extensiones)**
Datos del Certificado		
Versión (versión)	Entero Hexadecimal [V3] < 0x2 >(Representa la versión 3 del X.509)	
Serial (S*erial Number*)	Entero Hexadecimal <Asignado por la AC> (No negativo)	
Algoritmo de Firma (*signatureAlgorithm*)	Algoritmo Autorizado (OID de los algoritmo permitido sha256/384/512WithECDSAEncryption)	
Datos de Emisor (*issuer*)		
Nombre Común (*commonName*)	UTF8 <identificación de la AC principal O Subordinada> **(Requerido)**	

Departamento (*organizationalUnitName*)	UTF8 <División o unidad de la CA (ej. "Departamento de Emisión de Certificados")> **(Opcional)**	
Organización (*organizationName*)	UTF8 [Sistema Nacional de Certificación Electrónica] (Requerido)	
Localidad(*localityName*)	UTF8 <Dirección física del Emisor> (Opcional)	
Estado(*stateOrProvinceName*)	UTF8 <Estado en el cual se ubica el Emisor> (Opcional)	
País (*countryName*)	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*)	<Si la CA elige colocar el nombre completo se debe seguir las directrices de la CA browser Forum BR SMIME>	
Seudónimo(Pseudonym)	<Si contiene este campo es **Requerido** contener el Alias o sobrenombre verificado, los atributos Nombre y Apellido no deben estar presentes>	
Nombre (GivenName)	<Nombre del sujeto> (Si el CN es el Nombre Personal es **Requerido** que el certificado use atributos separados, y para este caso Seudónimo no debe estar presente)	
Apellido (Surname)	<Nombre del sujeto> (Si el CN es el Nombre Personal es **Requerido** que el certificado use atributos separados, y para este caso Seudónimo no debe estar presente)	
Nombre de la organización (organizationName)	<Debe contener el nombre legal verificado del patrocinador> **(Requerido)**	
Identificador de la organzación (organizacionIdentifier)	<Debe contener el identificador legal único del patrocinador, ej. Número de registro de información fiscal> **(Requerido)**	
Nombre de la unidad organizativa (organizationalUnitName)	<Unidad o departamento del patrocinador al que pertenece el individuo> **(Opcional)**	
Dirección de correo (emailAdress)	<La dirección de correo> Es O**pcional** en Subject DN, pero su presencia en la extensión SAN del presente certificado es **Requerido**>	
Titulo (title)	<Cargo que desempeña el titular del certificado> (Opcional)	
Serial (*serialNumber*)	Identificación fiscal o legal de la entidad **(Opcional)**	
Localidad (*localityName*)	UTF8<Ciudad de ubicación del titular> **(Opcional)**	
Estado (*stateOrProvinceName*)	UTF8 <Estado de ubicación del Titular> **(Opcional)**	

País (countryName)	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)	
NIST CURVE	P-*nnn* donde *nnn* puede ser 256, 384 o 521 **(Requerido)** Aplicar según la curva indicada en la longitud de la firma seleccionada en el "Algoritmo de Firma (*signatureAlgorithm*)"	
*** Para el caso de ECDSA se exigen los módulos anteriores**		
Extensiones		
Restricciones Básicas (basicConstraints) (Opcional)		
Autoridad de Certificación(aC)	Booleano [false]	
Uso de la llave (keyUsage) (Requerido)		
Firma digital	DigitalSignature(0) (**Requerido)**	
Compromiso de contenido (*contentCommitment*)	contentCommitment(1) - <Antes No Repudio - compromiso con el contenido firmado> (Requerido)	
Acuerdo de claves (keyAgreement)	<Para establecer claves de sesión para cifrado del contenido del correo> (Requerido)	
Identificador de clave de Autoridad Certificadora (Authority Key Identifier) (Requerido)		
Clave de Autoridad (*keyIdentifier*)	KeyIdentifier <Identificador de la clave pública de la AC> (Requerido)	
Identificador de la clave del sujeto (Subject Key Identifier) (Recomendable) RFC 5280		
Clave de Autoridad (*keyIdentifier*)	KeyIdentifier <clave pública del propio certificado de la AC>	
Nombre alternativo del sujeto (subjectAlternativeName) (Requerido)		
Formato de correo tradicional	Dirección de correo electrónico <Rfc822Name o SmtpUTF8Mailbox(RFC 9598)> (Requerido)	
Nombre del directorio (directoryname)	<GeneralName> (Opcional)	
Usos Extendidos de la Clave (extKeyUsage) (Requerido)		Definido por el emisor (RFC 5280 y RFC 9336)
Firma de documentos	Id-kp-documentSignin 1.3.6.1.4.1.311.10.3.12 (Requerido para firma de documentos)	
Protección de correo	Id-kp-emailProtection 1.3.6.1.5.5.7.3.4 (Requerido para s/mime)	
Puntos de Distribución de las LCR (cRLDistributionPoints) (Requerido)		

Punto de distribución LCR (*distributionPoint*)	<URL HTTP del servicio CRL de la AC>	
AIA (authorityInfoAccess) (Requerido)		
id-ad-ocsp	1.3.6.1.5.5.7.48.1 <URL HTTP del respondedor OCSP de la CA emisora (accessLocation)> (opcional)	
id-ad-caIssuers	1.3.6.1.5.5.7.48.2 <URL HTTP del certificado de la CA emisora (accessLocation)> (opcional, pero debería)	
Políticas de certificado (certificatePolicies)(Requerido)		
PolicyIdentifier (Identificador de política) Requerido		
policy identifier(s)	<Indica la política de la CA que confirma el cumplimiento>	
PolicyQualifiers (Calificador de política)		
cPSuri	<URL de la Declaración de Prácticas de Certificación (DPC/CPS) de la CA emisora>	
Firma		
Algoritmo de Firma (*signatureAlgorithm*)	Algoritmo Autorizado (OID de los algoritmos permitidos sha256/384/512WithECDSAEncryption)	
Firma(*signature*)	<Contenido de la Firma>	

7.10.16 Estructura de Certificado Electrónico para Control de Acceso Lógico

Certificado cuyo suscriptor es una persona jurídica o natural, 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. Su función principal es probar la identidad en un punto de acceso (lógico) para permitir o denegar la entrada a un sistema, red o aplicación. Perteneciente a la Validación Individual (IV) si el suscriptor es una persona natural y a la Organización validada (OV) si el suscriptor es una persona jurídica. Si requiere un control mas estricto de acceso y propiedad puede optar por Validación Extendida (EV) siguiendo las directrices de la CA Browser Forum TLS BR.

Control de Acceso Lógico		
Nombre(X.509)	**Tipo de dato [Constante] < Valor >**	**Crítica (para extensiones)**
Datos del Certificado		
Versión (versión)	Entero Hexadecimal [V3] < 0x2 >(Representa la versión 3 del X.509)	
Serial (*Serial Number*)	Entero Hexadecimal <Asignado por la AC> (No negativo)	

Algoritmo de Firma (*signatureAlgorithm*)	Algoritmo Autorizado (OID de los algoritmos permitidos sha256/384/512WithECDSAEncryption)	
Datos de Emisor (issuer)		
Nombre Común (*commonName*)	UTF8 <identificación de la AC principal O Subordinada> **(Requerido)**	
Departamento (*organizationalUnitName*)	UTF8 <División o unidad de la CA (ej. "Departamento de Emisión de Certificados")> **(Opcional)**	
Organización (*organizationName*)	UTF8 [Sistema Nacional de Certificación Electrónica] **(Requerido)**	
Localidad(*localityName*)	UTF8 <Dirección física del Emisor> **(Opcional)**	
Estado(*stateOrProvinceName*)	UTF8 <Estado en el cual se ubica el Emisor> **(Opcional)**	
País (*countryName*)	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*)		
Componente de dominio (domainComponent)	<Si esta presente requiere una etiqueta de dominio válida> **(Opcional y solo aplica para OV)**	
Apellido (surname)	<Apellido del titular> **(Requerido para IV, no aplica para OV)**	
Nombre de pila (givenName)	<Nombre del titular> (**Requerido para IV, no aplica para OV)**	
Organización (*organizationName*)	**UTF8 <**Nombre del titular y/o comercial>**(Requerido)**	
Localidad(*localityName*)	UTF8<Localidad del titular> **(Opcional)**	
Estado (*stateOrProvinceName*)	UTF8UTF8 <El nombre del titular y/o nombre comercial.> **[No recomendado para IV y Opcional para OV (Si falta el campo `localityName` es requerido Organización]**>	
País (*countryName*)	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)	
NIST CURVE	P-*nnn* donde *nnn* puede ser 256, 384 o 521 **(Requerido)** Aplicar según la curva indicada en la longitud de la firma seleccionada en el "Algoritmo de Firma (*signatureAlgorithm*)"	
*** Para el caso de ECDSA se exigen los módulos anteriores**		

Extensiones		
Restricciones Básicas (basicConstraints) (Opcional)		
Autoridad de Certificación(aC)	Booleano [false]	
Uso de la llave (keyUsage) (Requerido)		
Firma digital	digitalSignature(0)	
Acuerdo clave	KeyAgreement (opcional, pero no se recomienda)	
Identificador de clave de Autoridad Certificadora (Authority Key Identifier) (Requerido)		
Clave de Autoridad (keyIdentifier)	[0]KeyIdentifier <Identificador de la clave pública de la AC> (Requerido)	
Usos Extendidos de la Clave (extKeyUsage) (Requerido)		
Autenticación del servidor	serverAuth 1.3.6.1.5.5.7.3.1 (Requerido)	
Autenticación de cliente	ClientAuth 1.3.6.1.5.5.7.3.2 (Requerido)	
Nombre Alternativo del Titular (subjectAltName) (Requerido)		
Nombres de Dominio (dNSName)	<Sitio Web de la Empresa> (NO puede contener "Internal Names" (nombres reservados/internalos)	
Dirección IP válida (iPAddress)	<La entrada NO DEBE contener Una dirección IP reservada.>	
Puntos de Distribución de las LCR (cRLDistributionPoints) (Requerido)		
Punto de distribución LCR (*distributionPoint*)	<URL HTTP del servicio CRL de la AC>	
AIA (authorityInfoAccess) (Requerido)		
id-ad-ocsp	<URL HTTP del respondedor OCSP de la CA emisora (accessLocation)> (opcional)	
id-ad-caIssuers	1.3.6.1.5.5.7.48.2 <URL HTTP del certificado de la CA emisora (accessLocation)> (opcional, pero debería)	
Políticas de certificado (certificatePolicies)(Requerido)		
PolicyIdentifier (PC/CP) (Requerido)		
policyIdentifier(s)	<Indica la política de la CA que confirma el cumplimiento>	
PolicyQualifiers (DPC/CPS) (Opcional)		
cPSuri	<URL de la Declaración de Prácticas de Certificación (CPS) de la CA emisora>	
Firma		
Algoritmo de Firma (*signatureAlgorithm*)	Algoritmo Autorizado (OID de los algoritmos permitidos sha256/384/512WithECDSAEncryption)	
Firma(*signature*)	<Contenido de la Firma>	

7.10.17 Estructura de Certificado Electrónico para Firma de Transacción

Certificado emitido a nombre de una Persona Jurídica (empresa u organismo) o de su Representante Autorizado, cuyo propósito principal es garantizar la integridad y el no repudio de las transacciones electrónicas (órdenes de pago, transferencias de fondos, etc.) realizadas en el ámbito de la entidad. El enfoque está en los atributos que demuestran la identidad legal de la entidad suscriptora y/o la autoridad delegada del firmante. El siguiente perfil se ajusta a la validación de "Organización Validada", si requiere "Perfil validado por patrocinador" debe seguir las directrices de la CA Browser Forum SMIMEBR

Firma de Transacción		
Nombre(X.509)	**Tipo de dato [Constante] < Valor >**	**Crítica (para extensiones)**
Datos del Certificado		
Versión (versión)	Entero Hexadecimal [V3] < 0x2 >(Representa la versión 3 del X.509)	
Serial (*Serial Number*)	Entero Hexadecimal <Asignado por la AC> (No negativo)	
Algoritmo de Firma (*signatureAlgorithm*)	Algoritmo Autorizado (OID de los algoritmo permitido sha256/384/512WithECDSAEncryption)	
Datos de Emisor (*issuer*)		
Nombre Común (*commonName*)	UTF8 <identificación de la AC principal O Subordinada> **(Requerido)**	
Departamento (*organizationalUnitName*)	UTF8 <División o unidad de la CA (ej. "Departamento de Emisión de Certificados")> **(Opcional)**	
Organización (*organizationName*)	UTF8 [Sistema Nacional de Certificación Electrónica] **(Requerido)**	
Localidad(*localityName*)	UTF8 <Dirección física del Emisor> **(Opcional)**	
Estado (*stateOrProvinceName*)	UTF8 <Estado en el cual se ubica el Emisor> **(Opcional)**	
País (*countryName*)	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 <El nombre de la entidad que firma> **(Opcional)**	
Organización (*organizationName*)	UTF8 <El nombre legal de la organización> **(Requerido)**	

Identificador de organización (organizationIdentifier)	<Identificador legal único de la organización(ej. Número de Registro Único de información fiscal)> **(Requerido)**	
serialNumber (DN)	<Número de identificador único de la persona que usa el certificado> **(Opcional)**	
Departamento (*organizationalUnitName*)	UTF8<La unidad o departamento (útil para perfiles empresariales, ej. "Departamento legal")> **(Opcional)**	
Dirección de correo (emailAddress)	<La dirección de correo> Es **Opcional** en Subject DN, pero su presencia en la extensión SAN del presente certificado es **Requerido**>	
Localidad(*localityName*)	UTF8<Ciudad o localidad de la organización> **(Opcional)**	
Estado (*stateOrProvinceName*)	UTF8<Información del estado o provincia de la organización> **(Opcional)**	
País (*countryName*)	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)	
NIST CURVE	P-*nnn* donde *nnn* puede ser 256, 384 o 521 **(Requerido)** Aplicar según la curva indicada en la longitud de la firma seleccionada en el "Algoritmo de Firma (*signatureAlgorithm*)"	
*** Para el caso de ECDSA se exigen los módulos anteriores**		
Extensiones		
Restricciones Básicas (basicConstraints) (Opcional)		
Autoridad de Certificación(aC)	Booleano [false]	
Uso de la llave (keyUsage) (Requerido)		
Firma digital	DigitalSignature(0) **(Requerido)**	
Compromiso de contenido (*contentCommitment*)	contentCommitment(1) - <Antes No Repudio - compromiso con el contenido firmado> (Requerido)	
Acuerdo de claves (keyAgreement)	<Para establecer claves de sesión para cifrado del contenido del correo> (Requerido)	
Identificador de clave de Autoridad Certificadora (Authority Key Identifier) (Requerido)		
Clave de Autoridad (*keyIdentifier*)	KeyIdentifier <Identificador de la clave pública de la AC>(Requerido)	
Identificador de la clave del sujeto (Subject Key Identifier) (Recomendable) RFC 5280		
Clave de Autoridad (*keyIdentifier*)	KeyIdentifier <clave pública del propio certificado de la AC>	
Nombre alternativo del sujeto (subjectAlternativeName) (Requerido)		

Formato de correo tradicional	Dirección de correo electrónico <Rfc822Name o SmtpUTF8Mailbox(RFC 9598)> (Requerido)	
Nombre del directorio (directoryname)	<GeneralName> (Opcional)	
Usos Extendidos de la Clave (extKeyUsage) (Requerido)		Definido por el emisor (RFC 5280 y RFC 9336)
Firma de documentos	Id-kp-documentSignin 1.3.6.1.4.1.311.10.3.12	
Protección de correo	Id-kp-emailProtection 1.3.6.1.5.5.7.3.4 (Requerido para s/mime)	
Puntos de Distribución de las LCR (cRLDistributionPoints) (Requerido)		
Punto de distribución LCR (*distributionPoint*)	<URL HTTP del servicio CRL de la AC>	
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 certificado (certificatePolicies)(Requerido)		
PolicyIdentifier (Identificador de política) Requerido		
policy identifier(s)	<Indica la política de la CA que confirma el cumplimiento>	
PolicyQualifiers (Calificador de política)		
cPSuri	<URL de la Declaración de Prácticas de Certificación (DPC/CPS) de la CA emisora>	
Firma		
Algoritmo de Firma (*signatureAlgorithm*)	Algoritmo Autorizado (OID de los algoritmo permitido sha256/384/512WithECDSAEncryption)	
Firma(*signature*)	<Contenido de la Firma>	

7.10.18 Estructura de Certificado Electrónico para Factura Electrónica

Certificado cuyo suscriptor es una persona natural o jurídica, con el fin de emitir facturas electrónicas que garantizan la integridad y el no repudio. Es del tipo Firma de documentos que comparte tecnología base de S/MIME. El siguiente perfil es estructurado al tipo de validación “Patrocinador Validado” si requiere otra validación aplicada como “Individual validado” o “Organización validado” seguir las directrices de la CA Browser Forum S/MIMEBR.

Factura Electrónica

Nombre(X.509)	Tipo de dato [Constante] < Valor >	Crítica (para extensiones)
Datos del Certificado		
Versión (*versión*)	Entero Hexadecimal [V3] < 0x2 >(Representa la versión 3 del X.509)	
Serial (*Serial Number*)	Entero Hexadecimal <Asignado por la AC> (No negativo)	
Algoritmo de Firma (*signatureAlgorithm*)	Algoritmo Autorizado (OID de los algoritmos permitidos sha256/384/512WithECDSAEncryption)	
Datos de Emisor (*issuer*)		
Nombre Común (commonName)	UTF8 <identificación de la AC principal O Subordinada> **(Requerido)**	
Departamento (organizationalUnitName)	UTF8 <División o unidad de la CA (ej. "Departamento de Emisión de Certificados")> **(Opcional)**	
Organización (organizationName)	UTF8 [Sistema Nacional de Certificación Electrónica] **(Requerido)**	
Localidad (localityName)	UTF8 <Dirección física del Emisor> **(Opcional)**	
Estado (stateOrProvinceName)	UTF8 <Estado en el cual se ubica el Emisor> **(Opcional)**	
País (*countryName*)	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*)	<Si la CA elige colocar el nombre completo se debe seguir las directrices de la CA browser Forum BR SMIME>	
Seudónimo(Pseudonym)	<Si **CN** contiene como valor Seudónimo es **Requerido** contener el Alias o sobrenombre verificado y en un atributo aparte, para este caso los atributos Nombre y Apellido no deben estar presentes>	
Nombre (GivenName)	<Nombre del sujeto> (Si el CN es el Nombre Personal completo, es **Requerido** que el certificado use atributos separados, y para este caso Seudónimo no debe estar presente)	
Apellido (Surname)	<Nombre del sujeto> (Si el CN es el Nombre Personal completo, es **Requerido** que el certificado use atributos separados, y para este caso Seudónimo no debe estar presente)	
Nombre de la organización (organizationName)	<Debe contener el nombre legal verificado del patrocinador> **(Requerido)**	

Identificador de la organzación (organizacionIdentifier)	<Debe contener el identificador legal único del patrocinador, ej. Número de registro de información fiscal> **(Requerido)**	
Nombre de la unidad organizativa (organizationalUnitName)	<Unidad o departamento del patrocinador al que pertenece el individuo> **(Opcional)**	
Dirección de correo (emailAdress)	<La dirección de correo> Es O**pcional** en Subject DN, pero su presencia en la extensión SAN del presente certificado es **Requerido**>	
Título (title)	<El título o rol profesional> **(Requerido)**	
Serial (*serialNumber*)	UTF8 <El Número de Colegiado/Matrícula Profesional> **(Opcional)**	
Localidad (*localityName*)	UTF8<Ciudad de ubicación del titular> **(Opcional)**	
Estado (*stateOrProvinceName*)	UTF8 <Estado de ubicación del Titular> **(Opcional)**	
País (*countryName*)	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)	
NIST CURVE	P-*nnn* donde *nnn* puede ser 256, 384 o 521 **(Requerido)** Aplicar según la curva indicada en la longitud de la firma seleccionada en el "Algoritmo de Firma (*signatureAlgorithm*)"	
*** Para el caso de ECDSA se exigen los módulos anteriores**		
Extensiones		
Restricciones Básicas (basicConstraints) (Opcional)		
Autoridad de Certificación(aC)	Booleano [false]	
Uso de la llave (keyUsage) (Requerido)		
Firma digital	digitalSignature(0)	
Compromiso de contenido (*contentCommitment*)	contentCommitment(1) - <Antes No Repudio - compromiso con el contenido firmado> (Requerido)	
Acuerdo de claves (keyAgreement)	<Para establecer claves de sesión para cifrado del contenido del correo> (**Requerido**)	
Identificador de clave de Autoridad Certificadora (Authority Key Identifier)(Requerido)		
Clave de Autoridad (*keyIdentifier*)	[0]KeyIdentifier <Identificador de la clave pública de la AC emisora> (Opcional)	
Identificador de la clave del sujeto (Subject Key Identifier) (Recomendable) RFC 5280		
Clave de Autoridad (*keyIdentifier*)	KeyIdentifier <clave pública del propio certificado de la AC>	
Nombre alternativo del sujeto (subjectAlternativeName) (Requerido)		

Formato de correo tradicional	Dirección de correo electrónico <Rfc822Name o SmtpUTF8Mailbox(RFC 9598)> (Requerido)	
Nombre del directorio (directoryname)	<GeneralName> (Opcional)	
Usos Extendidos de la Clave (extKeyUsage) (Requerido)		Definido por el emisor (RFC 5280 y RFC 9336)
Firma de documentos	Id-kp-documentSignin 1.3.6.1.4.1.311.10.3.12	
Protección de correo	Id-kp-emailProtection 1.3.6.1.5.5.7.3.4 (Requerido para uso s/mime)	
Puntos de Distribución de las LCR (cRLDistributionPoints) (Requerido)		
Punto de distribución LCR (*distributionPoint*)	<URL HTTP del servicio CRL de la AC>	
AIA (authorityInfoAccess) (Requerido)		
id-ad-ocsp	1.3.6.1.5.5.7.48.1 <URL HTTP del respondedor OCSP de la CA emisora (accessLocation)> (opcional)	
id-ad-caIssuers	1.3.6.1.5.5.7.48.2 <URL HTTP del certificado de la CA emisora (accessLocation)> (opcional, pero debería)	
Políticas de certificado (certificatePolicies)(Requerido)		
PolicyIdentifier (Identificador de política) Requerido		
policy identifier(s)	<Indica la política de la CA que confirma el cumplimiento>	
PolicyQualifiers (Calificador de política)		
cPSuri	<URL de la Declaración de Prácticas de Certificación (DPC/CPS) de la CA emisora>	
Firma		
Algoritmo de Firma (*signatureAlgorithm*)	Algoritmo Autorizado (OID de los algoritmos permitidos sha256/384/512WithECDSAEncryption)	
Firma(*signature*)	<Contenido de la Firma>	

7.10.19 Estructura de Certificado Electrónico para Firma de Software

Certificado cuyo suscriptor es una persona natural o jurídica, 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 contenga información sobre ese software. Con la finalidad de asegurar la integridad del código y autenticar la identidad del editor o desarrollador. El siguiente perfil se estructura con Validación extendida (EV) y sin Validación extendida (Non-EV) de acuerdo a la CA Browser Forum Code Signing. Si solo requiere EV o Non-EV aparte seguir las directrices del estándar.

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 (*Serial Number*)	Entero Hexadecimal <Asignado por la AC> (No negativo)	
Algoritmo de Firma (*signatureAlgorithm*)	Algoritmo Autorizado (OID de los algoritmo permitido sha256/384/512WithECDSAEncryption)	
Datos de Emisor (*issuer*)		
Nombre Común (*commonName*)	UTF8 <identificación de la AC principal O Subordinada> **(Requerido)**	
Departamento (*organizationalUnitName*)	UTF8 <División o unidad de la CA (ej. "Departamento de Emisión de Certificados")> **(Opcional)**	
Organización (*organizationName*)	UTF8 [Sistema Nacional de Certificación Electrónica] **(Requerido)**	
Localidad(*localityName*)	UTF8 <Dirección física del Emisor> **(Opcional)**	
Estado (*stateOrProvinceName*)	UTF8 <Estado en el cual se ubica el Emisor> **(Opcional)**	
País (*countryName*)	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)	<Nombre legal del titular(natural o jurídica)> (**Requerido**)	
Organización (*organizationName*)	UTF8 <Nombre de la organización> **(Opcional pero, si se incluye, la información debe haber sido verificada por la AC)**	
Nombre del estado o provincia (stateOrProvinceName)	UTF8 <información del estado o provincia del titular> **(Opcional pero, si se incluye, la información debe haber sido verificada por la AC)**	
Departamento (*organizationalUnitName*)	UTF8<Nombre de la división interna de la organización(ej., Gerencia de desarrollo)> **(Opcional pero, si se incluye, la información debe haber sido verificada por la AC)**	

Nombre de la localidad (localityName)	UTF8<Información de la localidad del titular> **(Opcional(Opcional pero, si se incluye, la información debe haber sido verificada por la AC))**	
Codigo postal (postalCode)	UTF8<Código postal del sujeto> **(Opcional pero, si se incluye, la información debe haber sido verificada por la AC)**	
País (*countryName*)	UTF8 [VE] **(Opcional pero, si se incluye, la información debe haber sido verificada por la AC))**	
Información de Clave Pública del Titular (*subjectPublicKey*)		
Algoritmo de clave pública (*algorithm*)	<Algoritmo Asignado> (ecdsaEncryption, dhpublicnumber, id-ecdsa, id-ecdsaPublicKey)	
NIST CURVE	P-*nnn* donde *nnn* puede ser 256, 384 o 521 **(Requerido)** Aplicar según la curva indicada en la longitud de la firma seleccionada en el "Algoritmo de Firma (*signatureAlgorithm*)"	
*** Para el caso de ECDSA se exigen los módulos anteriores**		
Extensiones		
Restricciones Básicas (basicConstraints) (Opcional)		
Autoridad de Certificación(aC)	Booleano [false]	
Uso de la llave (keyUsage) (Requerido)		x
Firma digital	digitalSignature(0)	
Identificador de clave de Autoridad Certificadora (Authority Key Identifier) (Requerido)		
Clave de Autoridad (*keyIdentifier*)	[0]KeyIdentifier <Identificador de la clave pública de la AC emisora> (Requerido)	
Usos Extendidos de la Clave (extKeyUsage) (Opcional)		
Firma de código	Id-kp-codeSigning 1.3.6.1.5.5.7.3.3 (Requerido)	
Firma de por vida	Lifetime Signing OID (1.3.6.1.4.1.311.10.3.13) (Opcional)	
Protección de correo electrónico	Id-kp-emailProtection (Opcional)	
Firma de documentos	Document Signing 1.3.6.1.4.1.311.10.3.12 (Opcional)	
Puntos de Distribución de las LCR (*cRLDistributionPoints*) (Requerido)		
Punto de distribución LCR (*distributionPoint*)	<URL HTTP del servicio CRL de la AC>	
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 certificado (certificatePolicies)(Requerido)		

PolicyIdentifier (PC/CP) (Requerido)		
policyIdentifier(s)	<Indica la política de la CA que confirma el cumplimiento>	
PolicyQualifiers (DPC/CPS) (Opcional)		
cPSuri	<URL de la Declaración de Prácticas de Certificación (CPS) de la CA emisora>	
Firma		
Algoritmo de Firma (*signatureAlgorithm*)	Algoritmo Autorizado (OID de los algoritmo permitido sha256/384/512WithECDSAEncryption)	
Firma(*signature*)	<Contenido de la Firma>	

7.10.20 Estructura de Certificado Electrónico para Redes Virtuales Privadas (VPN)

Certificado cuyo suscriptor es una persona natural o jurídica, que permite que la conexión (túnel VPN) del servidor y el usuario sea segura, logrando el control y propiedad de una red privada o de una máquina específica en dicha red. Los tipos de validación que cubre la necesidad de verificar una identidad son Organización validada (OV) si es persona jurídica y Individual validado (IV) si es persona natural. Si requiere un control mas estricto de acceso y propiedad puede optar por Validación Extendida (EV) siguiendo las directrices de la CA Browser Forum TLS BR.

Redes Virtuales Privadas (VPN)		
Nombre(X.509)	**Tipo de dato [Constante] < Valor >**	**Crítica (para extensiones)**
Datos del Certificado		
Versión (versión)	Entero Hexadecimal [V3] < 0x2 >(Representa la versión 3 del X.509)	
Serial (*Serial Number*)	Entero Hexadecimal <Asignado por la AC> (No negativo)	
Algoritmo de Firma (*signatureAlgorithm*)	Algoritmo Autorizado (OID de los algoritmo permitido sha256/384/512WithECDSAEncryption)	
Datos de Emisor (*issuer*)		
Nombre Común (*commonName*)	UTF8 <identificación de la AC principal O Subordinada> **(Requerido)**	
Departamento (*organizationalUnitName*)	UTF8 <División o unidad de la CA (ej. "Departamento de Emisión de Certificados")> **(Opcional)**	
Organización (*organizationName*)	UTF8 [Sistema Nacional de Certificación Electrónica] (Requerido)	
Localidad(*localityName*)	UTF8 <Dirección física del Emisor> **(Opcional)**	
Estado(*stateOrProvinceName*)	UTF8 <Estado en el cual se ubica el Emisor> **(Opcional)**	
País (*countryName*)	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*)		
Componente de dominio (domainComponent)	Nombre de dominio del sitio web que protege el certificado **(opcional solo para OV, no debe estar para IV)** <No se permiten direcciones IP privadas>	
Apellido(surname)	<Apellido del titular> **(Requerido para IV, no debe estar para OV)**	
Nombre(givenName)	<Nombre del titular> **(Requerido para IV, no debe estar para OV)**	
Organización (*organizationName*)	UTF8 <El nombre y/o el nombre comercial del Sujeto> **(Requerido para OV, no debe estar para IV)**	
Localidad (*localityName*)	UTF8<Ciudad donde se ubica el titular o suscriptor del certificado> **(Opcional)**	
Estado (*stateOrProvinceName*)	UTF8<Información del estado o provincia del sujeto **(Opcional)** Si falta el campo `localityName` es requerido Organización**>**	
País (*countryName*)	UTF8 [VE] (ISO 3166-1-alpha-2) **(Requerido)**	
Localidad (*localityName*)	UTF8<Ciudad donde se ubica el titular o suscriptor del certificado> **(Opcional)**	
Información de Clave Pública del Titular (*subjectPublicKey*)		
Algoritmo de clave pública (*algorithm*)	<AlgoritmoAsignado>(ecdsaEncryption, dhpublicnumber,id-ecdsa, id-ecdsaPublicKey)	
NIST CURVE	P-*nnn* donde *nnn* puede ser 256, 384 o 521 **(Requerido)** Aplicar según la curva indicada en la longitud de la firma seleccionada en el "Algoritmo de Firma (*signatureAlgorithm*)"	
*** Para el caso de ECDSA se exigen los módulos anteriores**		
Extensiones		
Restricciones Básicas (*basicConstraints*) (Opcional)		
Autoridad de Certificación(aC)	Booleano [false]	
Uso de la llave (keyUsage) (Requerido)		
Firma digital	*DigitalSignature*(0) (Requerido)	
Acuerdo clave	KeyAgreement (opcional, pero no se recomienda)	
Identificador de clave de Autoridad Certificadora (Authority Key Identifier) (Requerido)		

Clave de Autoridad (*keyIdentifier*)Clave de Autoridad (keyIdentifier)	[0]KeyIdentifier <Identificador de la clave pública de la AC emisora> (Requerido)	
Usos Extendidos de la Clave (*extKeyUsage*) (Requerido)		
Autenticación del servidor	serverAuth 1.3.6.1.5.5.7.3.1 (Requerido)	
Autenticación de cliente	ClientAuth 1.3.6.1.5.5.7.3.2 (opcional)	
Nombre Alternativo del Titular (subjectAltName) (Requerido)		
Nombres de Dominio (dNSName)	<Sitio Web de la Empresa> (NO puede contener "Internal Names" (nombres reservados/internalos)	
Dirección IP válida (iPAddress)	<La entrada NO DEBE contener Una dirección IP reservada.>	
Puntos de Distribución de las LCR (cRLDistributionPoints) (Requerido)		
Punto de distribución LCR (*distributionPoint*)	<URL HTTP del servicio CRL de la AC>	
AIA (*authorityInfoAccess*) (Requerido)		
id-ad-ocsp	1.3.6.1.5.5.7.48.1 <URL HTTP del respondedor OCSP de la CA emisora (accessLocation)> (opcional)	
id-ad-calssuers	1.3.6.1.5.5.7.48.2 <URL HTTP del certificado de la CA emisora (accessLocation)> (opcional, pero debería)	
Políticas de certificado (certificatePolicies)(Requerido)		
PolicyIdentifier (PC/CP) (Requerido)		
policy identifier(s)	<Indica la política de la CA que confirma el cumplimiento>	
PolicyQualifiers (DPC/CPS) (Opcional)		
cPSuri	<URL de la Declaración de Prácticas de Certificación (CPS) de la CA emisora>	
Firma		
Algoritmo de Firma (*signatureAlgorithm*)	Algoritmo Autorizado (OID de los algoritmos permitidos mínimo sha256/384/512WithECDSAEncryption)	
Firma (*signature*)	<Contenido de la Firma>	

7.10.21 Estructura de Certificado Electrónico para SSL (Secure Sockets Layer)

Certificado cuyo suscriptor es una persona natural o jurídica, para autenticar la identidad de un sitio web y habilitar una conexión cifrada. Cuenta con Dominio Validado (DV) para los dos tipos de suscriptores y Organización Validada (OV) exclusivo para persona Jurídica. La elección depende de la confianza que el titular quiera transmitir a los usuarios en su sitio web. Importante recordar que un certificado con DV tiene el Sujeto con pocos atributos (quizás solo país), confía completamente en la extensión Subject Alternative Name (SAN) para identificar el sitio web. Si requiere un control mas estricto de acceso y propiedad puede

optar por Validación Extendida (EV) siguiendo las directrices de la CA Browser Forum TLS BR.

Certificado Electrónico SSL		
Nombre(X.509)	**Tipo de dato [Constante] < Valor >**	**Crítica (para extensiones)**
Datos del Certificado		
Versión (versión)	Entero Hexadecimal [V3] < 0x2 >(Representa la versión 3 del X.509)	
Serial (*Serial Number*)	Entero Hexadecimal <Asignado por la AC> (No negativo)	
Algoritmo de Firma (*signatureAlgorithm*)	Algoritmo Autorizado (OID de los algoritmo permitido sha256/384/512WithECDSAEncryption)	
Datos de Emisor (*issuer*)		
Nombre Común (*commonName*)	UTF8 <identificación de la AC principal O Subordinada> **(Requerido)**	
Departamento (*organizationalUnitName*)	UTF8 <División o unidad de la CA (ej. "Departamento de Emisión de Certificados")> **(Opcional)**	
Organización (*organizationName*)	UTF8 [Sistema Nacional de Certificación Electrónica] **(Requerido)**	
Localidad (*localityName*)	UTF8 <Dirección física del Emisor> **(Opcional)**	
Estado (*stateOrProvinceName*)	UTF8 <Estado en el cual se ubica el Emisor> **(Opcional)**	
País (*countryName*)	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)		
Componente de dominio (domainComponent)	Nombre de dominio del sitio web que protege el certificado **(opcional solo para OV)** <No se permiten direcciones IP privadas>	
Organización (*organizationName*)	UTF8 <El nombre y/o el nombre comercial del titurlar> **(Requerido solo para OV)**	
Localidad (*localityName*)	UTF8<Ciudad donde se ubica el titular o suscriptor del certificado> **(Opcional solo para OV)**	
Estado (*stateOrProvinceName*)	UTF8<Información del estado o provincia del sujeto **(Opcional solo para OV) Si falta el campo `localityName` es requerido Organización>**	
País (*countryName*)	UTF8 [VE] (ISO 3166-1-alpha-2) **(Puede estar para DV pero es Requerido OV)**	
Información de Clave Pública del Titular (*subjectPublicKey*)		

Algoritmo de clave pública (*algorithm*)	<Algoritmo Asignado> (ecdsaEncryption, dhpublicnumber, id-ecdsa, id-ecdsaPublicKey)	
NIST CURVE	P-*nnn* donde *nnn* puede ser 256, 384 o 521 **(Requerido)** Aplicar según la curva indicada en la longitud de la firma seleccionada en el "Algoritmo de Firma (*signatureAlgorithm*)"	
*** Para el caso de ECDSA se exigen los módulos anteriores**		
Extensiones		
Restricciones Básicas (*basicConstraints*) (Opcional)		
Autoridad de Certificación(aC)	Booleano [false]	
Uso de la llave (*keyUsage*) (Requerido)		
Firma digital	*DigitalSignature*(0) (Requerido)	
Acuerdo clave	KeyAgreement (opcional, pero no se recomienda)	
Identificador de clave de Autoridad Certificadora (Authority Key Identifier) (Requerido)		
Clave de Autoridad (keyIdentifier)	[0]KeyIdentifier <Identificador de la clave pública de la AC> (Requerido)	
Usos Extendidos de la Clave (*extKeyUsage*) (Requerido)		
Autenticación del servidor	serverAuth 1.3.6.1.5.5.7.3.1 (Requerido)	
Autenticación de cliente	ClientAuth 1.3.6.1.5.5.7.3.2 (opcional)	
Nombre Alternativo del Titular (subjectAltName) (Requerido)		
Nombres de Dominio (dNSName)	<Sitio Web de la Empresa> (NO puede contener "Internal Names" (nombres reservados/internalos)	
Dirección IP válida (iPAddress)	<La entrada NO DEBE contener Una dirección IP reservada.>	
Puntos de Distribución de las LCR (cRLDistributionPoints) (Requerido)		
Punto de distribución LCR (*distributionPoint)*	<URL HTTP del servicio CRL de la AC>	
AIA (*authorityInfoAccess*) (Requerido)		
id-ad-ocsp	1.3.6.1.5.5.7.48.1 <URL HTTP del respondedor OCSP de la CA emisora (accessLocation)> (opcional)	
id-ad-calssuers	1.3.6.1.5.5.7.48.2 <URL HTTP del certificado de la CA emisora (accessLocation)> (opcional, pero debería)	
Políticas de certificado (certificatePolicies)(Requerido)		
PolicyIdentifier (PC/CP) (Requerido)		
policy identifier(s)	<OID Autorizado por SUSCERTE> 1.3.6.1.5.5.7.14	
PolicyQualifiers (DPC/CPS) (Opcional)		
cPSuri	<URL de la Declaración de Prácticas de Certificación (CPS) de la CA emisora>	
Firma		

Algoritmo de Firma (*signatureAlgorithm*)	Algoritmo Autorizado (OID de los algoritmos permitidos sha256/384/512WithECDSAEncryption)	
Firma (*signature*)	<Contenido de la Firma>	