CAMERFIRMA COLOMBIA SAS CERTIFICADOS CERTIFICADO DE FUNCIÓN PÚBLICA EN TARJETA [12102]				
Campo	**Contenido**	**O**	**C**	**Estilo / Observaciones**
1. TBSCertificate				
1.1 Version	V3	√	X	[RFC5280]
1.2 Serial number	<proviene de la CA>	√	X	Establecido automáticamente por la Entidad de Certificación [18 bytes]
1.3 Signature Algorithm	sha256WithRSAEncryption	√	X	OID 1.2.840.113549.1.1.11
1.4 Issuer		√	X	
1.4.1 countryName (C)	Esta información proviene de la CA emisora	-	-	OID 2.5.4.6 [PRINTABLE STRING]
1.4.2 organizationName (O)	Esta información proviene de la CA emisora	-	-	OID 2.5.4.10 [UTF8 STRING]
1.4.3 organizationIdentifier	Esta información proviene de la CA emisora	-	-	ETSI EN 319 412-1 OID 2.5.4.97 [UTF8 STRING]
1.4.4 serialNumber (SN)	Esta información proviene de la CA emisora	-	-	OID 2.5.4.5 [PRINTABLE STRING]
1.4.5 stateOrProvinceName	Esta información proviene de la CA emisora	-	-	OID 2.5.4.8 [UTF8 STRING]
1.4.6 localityName (L)	Esta información proviene de la CA emisora	-	-	OID 2.5.4.7 [UTF8 STRING]
1.4.7 commonName (CN)	Esta información proviene de la CA emisora	-	-	OID 2.5.4.3 [UTF8 STRING]
1.5 Validity	1 año	√	X	
1.5.1 notBefore	<a incorporar cuando se emita el certificado>	√	-	UTC Time
1.5.2 notAfter	<a incorporar cuando se emita el certificado>	√	-	UTC Time
1.6 Subject		√	X	
1.6.1 countryName (C)	CO	√	-	OID 2.5.4.6 [PRINTABLE STRING]
1.6.2 organizationName (O)	Organización del suscriptor	√	-	Empresa titular del certificado. Nombre legal del suscriptor del certificado. OID 2.5.4.10 [UTF8 STRING]
1.6.3 organizationIdentifier	Identificación de la entidad suscriptora del certificado	√	-	"NIT" + "CO" + "-" + <NIT de la entidad suscriptora> [ETSI EN 319 412-1] P.Ej.:"NITCO-901312112-4" OID 2.5.4.97 [UTF8 STRING]
1.6.4 organizationalUnitName (OU)	Departamento en la organización del suscriptor	X	-	Área / Departamento / Unidad de trabajo OID 2.5.4.11

				[UTF8 STRING]
1.6.5 Title	Cargo del suscriptor en la organización	X	-	Puesto o cargo del empleado que lo vincula con la organización OID 2.5.4.12 [UTF8 STRING]
1.6.6 Locality	Municipio / Ciudad de la organización del suscriptor	√	-	OID 2.5.4.7 [UTF8 STRING]
1.6.7 stateOrProvinceName	Estado / Departamento de la organización del suscriptor	√	-	Unidades territoriales OID 2.5.4.8 [UTF8 STRING]
1.6.8 streetAddress	Dirección de la organización del suscriptor	√	-	OID 2.5.4.9 [UTF8 STRING]
1.6.7 1.3.6.1.4.1.17326.30.11	Tipo de documento del suscriptor	√	-	NIT - Número de Identificación Tributaria CC - Cédula de Ciudadanía CE - Cédula de Extranjería TI - Tarjeta de Identidad PAS - Pasaporte SEG - Tarjeta Social Security ESN - Sociedad Extranjera sin NIT RC - Registro Civil CD - Carnet Diplomático OID 1.3.6.1.4.1.17326.30.11 [UTF8 STRING]
1.6.10 serialNumber (SN)	Número de documento del suscriptor	√	-	OID 2.5.4.5 [PRINTABLE STRING]
1.6.11 Given Name	Nombres del suscriptor	√	-	NOMBRE1 NOMBRE2 (en mayúsculas) OID 2.5.4.42 [UTF8 STRING]
1.6.12 Surname	Apellidos del suscriptor	√	-	APELLIDO1 APELLIDO2 (en mayúsculas) OID 2.5.4.4 [UTF8 STRING]
1.6.13 commonName (CN)	Nombre y apellidos del suscriptor	√	-	APELLIDO1 APELLIDO2 NOMBRE1 NOMBRE2 (en mayúsculas y sin separadores entre los apellidos y los nombres) OID 2.5.4.3 [UTF8 STRING]
1.6.14 description	“CERTIFICADO DE FUNCIÓN PÚBLICA - EMITIDO POR CAMERFIRMA COLOMBIA SAS”	√	-	OID 2.5.4.13 [UTF8 STRING]

1.7 Subject Public Key Info	rsaEncryption	√	X	Clave pública de 2048 bits [RFC3279] OID 1.2.840.113549.1.1.1
1.8 Extensions				
1.8.1 Standard Extensions				
1.8.1.1 Authority Key Identifier		√	X	OID 2.5.29.35
1.8.1.1.1 keyIdentifier	<a incorporar cuando se emita el certificado>	-	-	
1.8.1.1.2 authorityCertIssuer	<a incorporar cuando se emita el certificado>	-	-	
1.8.1.1.3 authorityCertSerialNumber	<a incorporar cuando se emita el certificado>	-	-	
1.8.1.2 Subject Key Identifier	<a incorporar cuando se emita el certificado>	√	X	OID 2.5.29.14
1.8.1.3 Key Usage		√	√	OID 2.5.29.15
1.8.1.3.1 digitalSignature	Seleccionado “1”	√	-	
1.8.1.3.2 contentCommitment	Seleccionado “1”	√	-	
1.8.1.3.3 keyEncipherment	No seleccionado “0”	X	-	
1.8.1.3.4 dataEncipherment	No seleccionado “0”	X	-	
1.8.1.3.5 keyAgreement	No seleccionado “0”	X	-	
1.8.1.3.6 keyCertSign	No seleccionado “0”	X	-	
1.8.1.3.7 cRLSign	No seleccionado “0”	X	-	
1.8.1.3.8 encipherOnly	No seleccionado “0”	X	-	
1.8.1.3.9 decipherOnly	No seleccionado “0”	X	-	
1.8.1.4 Certificate Policies		√	X	OID 2.5.29.32
1.8.1.4.1 Policy Identifier	OID de la política	√	-	1.3.6.1.4.1.17326.20.10.2.2
1.8.1.4.2 Policy Qualifier ID		√	-	
1.8.1.4.2.1 CPS Pointer	URI:https://policy.camerfirma.co	√	-	OID 1.3.6.1.5.5.7.2.1
1.8.1.4.2.2 User Notice	No está presente	X	X	
1.8.1.4.3 Policy Identifier 2	OID de la política [ETSI EN 319 411 1 - NCP+]	√	-	OID 0.4.0.2042.1.2
1.8.1.5 Subject Alternative Name	Correo electrónico del suscriptor	√	-	rfc822Name OID 2.5.29.17
1.8.1.6 Issuer Alternative Name	info@camerfirma.co	X	X	OID 2.5.29.18
1.8.1.7 Subject Directory Attributes	No está presente	X	-	OID 2.5.29.9
1.8.1.7.1 countryOfCitizenship	No está presente	X	-	OID 1.3.6.1.5.5.7.9.4
1.8.1.7.2 countryOfResidence	No está presente	X	-	OID 1.3.6.1.5.5.7.9.5
1.8.1.8 Basic Constraints		√	√	OID 2.5.29.19
1.8.1.8.1 cA	FALSE	√	-	
1.8.1.8.2 pathLenConstraint	0	√	-	
1.8.1.9 Name Constraints	No está presente	X	-	
1.8.1.10 Policy Constraints	No está presente	X	-	
1.8.1.11 Extended Key Usage		√	X	OID 2.5.29.37
1.8.1.11.1 serverAuth	No seleccionado “0”	X	-	OID 1.3.6.1.5.5.7.3.1
1.8.1.11.2 clientAuth	Seleccionado “1”	√	-	OID 1.3.6.1.5.5.7.3.2
1.8.1.11.3 codeSigning	No seleccionado “0”	X	-	OID 1.3.6.1.5.5.7.3.3
1.8.1.11.4 emailProtection	Seleccionado “1”	√	-	OID 1.3.6.1.5.5.7.3.4
1.8.1.11.5 timeStamping	No seleccionado “0”	X	-	OID 1.3.6.1.5.5.7.3.8
1.8.1.11.6 OCSPSigning	No seleccionado “0”	X	-	OID 1.3.6.1.5.5.7.3.9
1.8.1.11.7 Microsoft Smart Card Logon for Windows	No seleccionado “0”	X	-	OID 1.3.6.1.4.1.311.20.2.2

1.8.1.11.8 Microsoft Commercial Code Signing	No seleccionado “0”	X	-	OID 1.3.6.1.4.1.311.2.1.22
1.8.1.11.9 Microsoft Encrypting File System	No seleccionado “0”	X	-	OID 1.3.6.1.4.1.311.10.3.4
1.8.1.12 CRL Distribution Points		√	X	OID 2.5.29.31
1.8.1.12.1 CRL Distribution Point 1	http://crl.camerfirma.co/CAMERFIRMA_COLOMBIA_SAS_CERTIFICADOS_002.crl	√	-	
1.8.1.12.2 CRL Distribution Point 2	http://crl1.camerfirma.co/CAMERFIRMA_COLOMBIA_SAS_CERTIFICADOS_002.crl	√	-	
1.8.1.13 qcStatements	No está presente	X	-	OID 1.3.6.1.5.5.7.1.3
1.8.1.14 Netscape Cert Type	No está presente	X	-	
1.8.1.15 biometricInfo	No está presente	X	-	
1.8.1.16 Inhibit Any-Policy	No está presente	X	-	
1.8.1.17 Freshest CRL	No está presente	X	-	
1.8.2 Internet Certificate Extensions				
1.8.2.1 Authority Information Access		√	X	OID 1.3.6.1.5.5.7.1.1
1.8.2.1.1.1 accessMethod	id-ad-caIssuers	√	X	
1.8.2.1.1.2 accessLocation	Esta información proviene de la CA emisora	√	X	
1.8.2.1.2.1 accessMethod	id-ad-ocsp	√	X	
1.8.2.1.2.2 accessLocation	URI:http://ocsp.co.camerfirma.com	√	X	
1.8.2.2 Subject Information Access	No está presente	X	X	
2. PKCS#12				
2.1 Friendly Name	No está presente	X	X	

O = Obligatorio
C = Critico