Contenido

1. CERTIFICADO DE PERTENENCIA EMPRESA HARDWARE / FIRMA CENTRALIZADA

CERTIFICADO DE PERTENENCIA EMPRESA HARDWARE / FIRMA CENTRALIZADA				
Campo	**Contenido**	**Obligatorio**	**Crítico**	**Observaciones**
1 TBSCertificate				
1.1 Versión	V3	√	X	[RFC5280]
1.2 Serial number		√	X	Asignado por la plataforma al momento de generar el certificado
1.3 Signature algorithm	Sha256RSA	√	X	OID 1.2.840.113549.1.1.11

1.4 Signature hash algorithm	SHA256	√	X	
2 Issuer				
2.1 Email (E)	ca@gse.co	√	-	
2.2 Common Name (CN)	GSE SUB001_CO	√	X	OID 2.5.4.3
2.3 Organization	GESTION DE SEGURIDAD ELECTRONICA S.A. - GSE	√	-	OID 2.5.4.10
2.4 Serial Number	9002042728	√	-	OID 2.5.4.5
2.5 Organizational Unit	Internet Certification Authority http://www.gse.co	√	-	OID 2.5.4.11
2.6 Title	Subordinate Certificate			OID 2.5.4.12
2.7 StreetAddress	http://www.gse.co/address	√	-	OID 2.5.4.9
2.8 Locality	BOGOTÁ, D.C.	√	-	OID 2.5.4.7
2.9 Country	CO	√	X	OID 2.5.4.6
2.10 Description	GSE Subordinate Certificate 001 Colombia HW-KUSU	√	-	OID 2.5.4.13
3 Validity				
3.1 notBefore		√	X	Asignado por la plataforma al momento de generar el certificado - UTC Time - 5
3.2 notAfter		√	X	Asignado por la plataforma al momento de generar el certificado - UTC Time - 5
4 Subject				
4.1 Description	Certificado de Pertenencia a Empresa - Emitido por GSE SUB001_CO	√	-	OID 2.5.4.13
4.2 Common Name (CN)	Nombre y apellidos del suscriptor	√	-	OID 2.5.4.3 APELLIDO1 APELLIDO2 NOMBRE1 NOMBRE2 (en mayúsculas sin separadores entre los apellidos y los nombres)

4.3 1.3.6.1.4.1.31136.2.2.1.2.1	Tipo de Identificación Personal	√	-	Tipo de Identificación Personal
4.4 Serial Number	Número de documento del suscriptor	√	-	OID 2.5.4.5 Numero de documento
4.5 Email Address	Email del suscriptor	√	-	Email del suscriptor
4.6 Organization	Razón Social de la organización del suscriptor	√	-	OID 2.5.4.10 Nombre o Razón social de la empresa
4.7 1.3.6.1.4.1.31136.2.2.1.2.2	Tipo de Identificación de la Empresa	√	-	Tipo de Identificación de la Empresa
4.8 1.3.6.1.4.1.31136.2.2.1.2.3	Número de Identificación de la Empresa	√	-	Número de Identificación de la Empresa
4.9 1.3.6.1.4.1.31136.2.2.1.2.4	Entidad donde se registra la empresa	√	-	(Opcional) Entidad encargada de registrar la empresa ejemplo Cámara de comercio, superintendencia, etc.
4.10 Title	Cargo del suscriptor en la organización	√	-	OID 2.5.4.12 Cargo del Suscriptor
4.11 Organizational Unit (OU)	Departamento de la organización del suscriptor	√	-	OID 2.5.4.11 Dependencia en la empresa
4.12 StreetAddress	Dirección de la Organización	√	-	OID 2.5.4.9 Dirección de la empresa
4.13 StateOrProvinceName	Estado / Departamento de la organización del suscriptor	√	-	OID 2.5.4.8 Departamento / Estado de la empresa
4.14 Locality	Municipio / Ciudad de la organización Suscriptor	√	-	OID 2.5.4.7 Municipio / ciudad de la empresa
4.15 Surname	Apellidos del suscriptor	√	-	OID 2.5.4.4 APELLIDO1 APELLIDO2 (en mayúsculas sin separadores entre los apellidos)
4.16 Given Name	Nombre de suscriptor	√	-	OID 2.5.4.42 NOMBRE1 NOMBRE2 (en mayúsculas sin separadores entre los nombres)
4.17 Country	Nacionalidad del Suscriptor	√	-	OID 2.5.4.6 Nacionalidad del Suscriptor; Código de país de dos dígitos según ISO 3166-1.

4.18 Subject Publica Key Info	RSAEncryption Clave Pública de 2048 bits (RF3279) Clave Pública de 2048 bits (RF3279)	√	X	OID 1.2.840.113549.1.1.1 Clave pública de 2048 bits [RFC3279]
4.19 Public key parameters	"0500"	√	X	
5 Extensions				
5.1 Standard Extensions				
5.1.1 Authority Key Identifier	KeyID=8e 4a 03 5e a3 fd 09 a7 63 b5 64 ee 75 46 7a 6c dd be 45 49	√	X	OID 2.5.29.35
5.1.1.1 keyIdentifier		√	-	
5.1.1.2 authorityCertIssuer		√	-	
5.1.1.3 authorityCertSerialNumber		√	-	
5.1.2 Subject Key Identifier		√	-	OID 2.5.29.14
5.1.3 Key Usage		√	-	OID 2.5.29.15
5.1.3.1 digitalSignature	"1"	X	-	
5.1.3.2 nonRepudiation-ContentCommitment	"1"	X	-	
5.1.3.3 keyEncipherment	"1"	X	-	
5.1.3.4 dataEncipherment	"1"	X	-	
5.1.3.5 keyAgreement	"1"	X	-	

5.1.3.6 keyCertSign	"0"	√	-	
5.1.3.7 cRLSign	"0"	√	-	
5.1.3.8 encipherOnly	"0"	X	-	
5.1.3.9 decipherOnly	"0"	X	-	
5.1.4 Certificate Policies		√	X	OID 2.5.29.32
5.1.4.1 Policy Identifier	1.3.6.1.4.1.31136.2.2.3.2.2 - en token 1.3.6.1.4.1.31136.2.2.3.2.3 - En HSM	√	-	OID Definido por ECD GSE
5.1.4.2 Policy Qualifier ID		√	-	
5.1.4.2.1 CPS Pointer	http://cps.gse.co/sub/cps_sub001_ca_gse.pdf	√	-	OID 1.3.6.1.5.5.7.2.1
5.1.4.2.2 User Notice	Terms of use at CPS CA GSE http://cps.gse.co/sub/cps_sub001_ca_gse.pdf	√	-	
5.1.5 Subject Alternative Name				
5.1.6 Issuer Alternative Name	URI:http://www.gse.co	√	X	OID 2.5.29.18
5.1.7 Subject Directory Attributes	No está presente	X	X	OID 2.5.29.9
5.1.8 Basic Constraints		√	√	
5.1.8.1 cA	End Entity	√	-	
5.1.8.2 pathLenConstraint	No está presente	√	-	

5.1.9 Name Constraints	No está presente	X	X	
5.1.10 Policy Constraints	No está presente	X	X	
5.1.11 Extended Key Usage	No está presente	X	X	OID 2.5.29.37
5.1.11.1 serverAuth	"0"	-	-	OID 1.3.6.1.5.5.7.3.1
5.1.11.2 clientAuth	"1"	-	-	OID 1.3.6.1.5.5.7.3.2
5.1.11.3 codeSigning	"0"	-	-	OID 1.3.6.1.5.5.7.3.3
5.1.11.4 emailProtection	"1"	-	-	OID 1.3.6.1.5.5.7.3.4
5.1.11.5 timeStamping	"0"	-	-	OID 1.3.6.1.5.5.7.3.8
5.1.11.6 OCSPSigning	"0"	-	-	OID 1.3.6.1.5.5.7.3.9
5.1.11.7 Microsoft Smart Card Logon for Windows 1.3.6.2.1.311.20.2.2	"1"	-	-	OID 1.3.6.1.4.1.311.20.2 .2
5.1.11.8 Microsoft Commercial Code Signing 1.3.6.2.1.311.2.1.22	"0"	-	-	OID 1.3.6.1.4.1.311.2.1. 22
5.1.11.9 Microsoft Encrypting File System 1.3.6.2.1.31136.10.3.4	"1"	-	-	OID 1.3.6.1.4.1.311.10.3 .4
5.1.12 CRL Distribution Points		√	-	OID 2.5.29.31

5.1.12.1 CRL Distribution Point 1	URL= http://crl.gse.co/sub/crl_gse_sub001_sha2.crl	√	-	
5.1.12.2 CRL Distribution Point 2	URL= http://crl1.gse.co/sub/crl_gse_sub001_sha2.crl	√	-	
5.1.13 qcStatements	No esta presente	-	-	OID 1.3.6.1.5.5.7.1.3
5.1.13.1 id-etsi-qcs-QcCompliance	No está presente	-	-	
5.1.13.2 id-etsi-qcs-QcLimitValue	No está presente	-	-	
5.1.13.3 id-etsi-qcs-QcSSCD	No está presente	-	-	
5.1.14 Netscape Cert Type	No está presente	√	-	
5.1.15 Netscape Revocation URL	No está presente	-	-	
5.1.16 Netscape CA Policy URL	No está presente	-	-	
5.1.17 Netscape Comment	No está presente	-	-	
5.1.18 biometricInfo	No está presente	-	-	
5.1.19 Inhibit Any-Policy	No está presente	-	-	
5.1.20 Freshest CRL	No está presente	-	-	
5.2 Internet Certificate Extensions				
5.2.1 Authority Information Access 1		√	-	OID 1.3.6.1.5.5.7.1.1
5.2.1.1 accessMethod	Certification Authority Issuer (1.3.6.1.5.5.7.48.2)	√	-	

5.2.1.2 accessLocation	URI:http://certs.gse.co/sub/crt_gse_sub001_sha2.crt	√	-	
5.2.2 Authority Information Access 2				
5.2.2.1 accessMethod	On-line Certificate Status Protocol (1.3.6.1.5.5.7.48.1)	-	-	
5.2.2.2 accessLocation	URI:http://ocsp.gse.co	-	-	
5.2.3 Subject Information Access	No está presente	-	-	
6 PKCS#12				
6.1. Friendly Name		-	-	Asignado por la plataforma al momento de generar el certificado. SERIAL NUMBER GIVEN NAME SURNAME
7 Huella Digital				
7.1 Thumbprint algorithm	SHA1	√	X	
7.2 Thumbprint		√	X	Asignado por la plataforma al momento de generar el certificado

2. CERTIFICADO DE REPRESENTACION EMPRESA HARDWARE / FIRMA CENTRALIZADA

CERTIFICADO DE REPRESENTACION EMPRESA HARDWARE / FIRMA CENTRALIZADA				
Campo	**Contenido**	**Obligatorio**	**Crítico**	**Observaciones**
1 TBSCertificate				
1.1 Versión	V3	√	X	[RFC5280]
1.2 Serial number		√	X	Asignado por la plataforma al momento de generar el certificado
1.3 Signature algorithm	Sha256RSA	√	X	OID 1.2.840.113549.1.1.11
1.4 Signature hash algorithm	SHA256	√	X	
2 Issuer				
2.1 Email (E)	ca@gse.co	√	-	
2.2 Common Name (CN)	GSE SUB001_CO	√	X	OID 2.5.4.3
2.3 Organization	GESTION DE SEGURIDAD ELECTRONICA S.A. - GSE	√	-	OID 2.5.4.10
2.4 Serial Number	9002042728	√	-	OID 2.5.4.5
2.5 Organizational Unit	Internet Certification Authority http://www.gse.co	√	-	OID 2.5.4.11
2.6 Title	Subordinate Certificate			OID 2.5.4.12
2.7 StreetAddress	http://www.gse.co/address	√	-	OID 2.5.4.9
2.8 Locality	BOGOTÁ, D.C.	√	-	OID 2.5.4.7
2.9 Country	CO	√	X	OID 2.5.4.6
2.10 Description	GSE Subordinate Certificate 001 Colombia HW-KUSU	√	-	OID 2.5.4.13
3 Validity				

3.1 notBefore		√	X	Asignado por la plataforma al momento de generar el certificado - UTC Time - 5
3.2 notAfter		√	X	Asignado por la plataforma al momento de generar el certificado - UTC Time - 5
4 Subject				
4.1 Description	Certificado de Representación de Empresa - Emitido por GSE SUB001_CO	√	-	OID 2.5.4.13
4.2 Common Name (CN)	Nombre y apellidos del suscriptor (Representante Legal)	√	-	OID 2.5.4.3 APELLIDO1 APELLIDO2 NOMBRE1 NOMBRE2 (en mayúsculas sin separadores entre los apellidos y los nombres)
4.3 1.3.6.1.4.1.31136.2.2.1.2.1	Tipo de Identificación Personal	√	-	Tipo de Identificación Personal
4.4 Serial Number	Número de documento del suscriptor (Representante Legal)	√	-	OID 2.5.4.5 Numero de documento
4.5 Email Address	Email del suscriptor	√	-	Email del suscriptor
4.6 Organization	Razón Social de la organización del suscriptor	√	-	OID 2.5.4.10 Nombre o Razón social de la empresa
4.7 1.3.6.1.4.1.31136.2.2.1.2.2	Tipo de Identificación de la Empresa	√	-	Tipo de Identificación de la Empresa
4.8 1.3.6.1.4.1.31136.2.2.1.2.3	Número de Identificación de la Empresa	√	-	Número de Identificación de la Empresa
4.9 1.3.6.1.4.1.31136.2.2.1.2.4	Entidad donde se registra la empresa	√	-	(Opcional) Entidad encargada de registrar la empresa ejemplo Cámara de comercio, superintendencia, etc.
4.10 Title	Cargo del suscriptor en la organización	√	-	OID 2.5.4.12 Cargo del Suscriptor
4.11 StreetAddress	Dirección de la Organización	√	-	OID 2.5.4.9 Dirección de la empresa
4.12 StateOrProvinceName	Estado / Departamento de la organización del suscriptor	√	-	OID 2.5.4.8 Departamento / Estado de la empresa

4.13 Locality	Municipio / Ciudad de la organización Suscriptor	√	-	OID 2.5.4.7 Municipio / ciudad de la empresa
4.14 Surname	Apellidos del suscriptor	√	-	OID 2.5.4.4 APELLIDO1 APELLIDO2 (en mayúsculas sin separadores entre los apellidos)
4.15 Given Name	Nombre de suscriptor	√	-	OID 2.5.4.42 NOMBRE1 NOMBRE2 (en mayúsculas sin separadores entre los nombres)
4.16 Country	Nacionalidad del Suscriptor	√	-	OID 2.5.4.6 Nacionalidad del Suscriptor; Código de país de dos dígitos según ISO 3166-1.
4.17 Subject Publica Key Info	RSAEncryption Clave Pública de 2048 bits (RF3279) Clave Pública de 2048 bits (RF3279)	√	X	OID 1.2.840.113549.1.1.1 Clave pública de 2048 bits [RFC3279]
4.18 Public key parameters	"0500"	√	X	
5 Extensions				
5.1 Standard Extensions				
5.1.1 Authority Key Identifier	KeyID=8e 4a 03 5e a3 fd 09 a7 63 b5 64 ee 75 46 7a 6c dd be 45 49	√	X	OID 2.5.29.35
5.1.1.1 keyIdentifier		√	-	
5.1.1.2 authorityCertIssuer		√	-	
5.1.1.3 authorityCertSerialNumber		√	-	
5.1.2 Subject Key Identifier		√	-	OID 2.5.29.14
5.1.3 Key Usage		√	-	OID 2.5.29.15
5.1.3.1 digitalSignature	"1"	X	-	

5.1.3.2 nonRepudiation-ContentCommitment	"1"	X	-	
5.1.3.3 keyEncipherment	"1"	X	-	
5.1.3.4 dataEncipherment	"1"	X	-	
5.1.3.5 keyAgreement	"1"	X	-	
5.1.3.6 keyCertSign	"0"	√	-	
5.1.3.7 cRLSign	"0"	√	-	
5.1.3.8 encipherOnly	"0"	X	-	
5.1.3.9 decipherOnly	"0"	X	-	
5.1.4 Certificate Policies		√	X	OID 2.5.29.32
5.1.4.1 Policy Identifier	1.3.6.1.4.1.31136.2.2.3.3.2 - En token 1.3.6.1.4.1.31136.2.2.3.3.3 - En HSM	√	-	OID Definido por ECD GSE
5.1.4.2 Policy Qualifier ID		√	-	
5.1.4.2.1 CPS Pointer	http://cps.gse.co/sub/cps_sub001_ca_gse.pdf	√	-	OID 1.3.6.1.5.5.7.2.1
5.1.4.2.2 User Notice	Terms of use at CPS CA GSE http://cps.gse.co/sub/cps_sub001_ca_gse.pdf	√	-	
5.1.5 Subject Alternative Name				
5.1.6 Issuer Alternative Name	URI:http://www.gse.co	√	X	OID 2.5.29.18

5.1.7 Subject Directory Attributes	No está presente	X	X	OID 2.5.29.9
5.1.8 Basic Constraints		√	√	
5.1.8.1 cA	End Entity	√	-	
5.1.8.2 pathLenConstraint	No está presente	√	-	
5.1.9 Name Constraints	No está presente	X	X	
5.1.10 Policy Constraints	No está presente	X	X	
5.1.11 Extended Key Usage	No está presente	X	X	OID 2.5.29.37
5.1.11.1 serverAuth	"0"	-	-	OID 1.3.6.1.5.5.7.3.1
5.1.11.2 clientAuth	"1"	-	-	OID 1.3.6.1.5.5.7.3.2
5.1.11.3 codeSigning	"0"	-	-	OID 1.3.6.1.5.5.7.3.3
5.1.11.4 emailProtection	"1"	-	-	OID 1.3.6.1.5.5.7.3.4
5.1.11.5 timeStamping	"0"	-	-	OID 1.3.6.1.5.5.7.3.8
5.1.11.6 OCSPSigning	"0"	-	-	OID 1.3.6.1.5.5.7.3.9
5.1.11.7 Microsoft Smart Card Logon for Windows 1.3.6.2.1.311.20.2.2	"1"	-	-	OID 1.3.6.1.4.1.311.20.2 .2

5.1.11.8 Microsoft Commercial Code Signing 1.3.6.2.1.311.2.1.22	"0"	-	-	OID 1.3.6.1.4.1.311.2.1. 22
5.1.11.9 Microsoft Encrypting File System 1.3.6.2.1.31136.10.3.4	"1"	-	-	OID 1.3.6.1.4.1.311.10.3 .4
5.1.12 CRL Distribution Points		√	-	OID 2.5.29.31
5.1.12.1 CRL Distribution Point 1	URL=http://crl.gse.co/sub/crl_gse_sub001_sha2.crl	√	-	
5.1.12.2 CRL Distribution Point 2	URL=http://crl1.gse.co/sub/crl_gse_sub001_sha2.crl	√	-	
5.1.13 qcStatements	No está presente	-	-	OID 1.3.6.1.5.5.7.1.3
5.1.13.1 id-etsi-qcs-QcCompliance	No está presente	-	-	
5.1.13.2 id-etsi-qcs-QcLimitValue	No está presente	-	-	
5.1.13.3 id-etsi-qcs-QcSSCD	No está presente	-	-	
5.1.14 Netscape Cert Type	No está presente	√	-	
5.1.15 Netscape Revocation URL	No está presente	-	-	
5.1.16 Netscape CA Policy URL	No está presente	-	-	
5.1.17 Netscape Comment	No está presente	-	-	
5.1.18 biometricInfo	No está presente	-	-	

5.1.19 Inhibit Any-Policy	No está presente	-	-	
5.1.20 Freshest CRL	No está presente	-	-	
5.2 Internet Certificate Extensions				
5.2.1 Authority Information Access 1		√	-	OID 1.3.6.1.5.5.7.1.1
5.2.1.1 accessMethod	Certification Authority Issuer (1.3.6.1.5.5.7.48.2)	√	-	
5.2.1.2 accessLocation	URI:http://certs.gse.co/sub/crt_gse_sub001_sha2.crt	√	-	
5.2.2 Authority Information Access 2		-	-	
5.2.2.1 accessMethod	On-line Certificate Status Protocol (1.3.6.1.5.5.7.48.1)	-	-	
5.2.2.2 accessLocation	URI:http://ocsp.gse.co	-	-	
5.2.3 Subject Information Access	No está presente	-	-	
6 PKCS#12				
6.1. Friendly Name		-	-	Asignado por la plataforma al momento de generar el certificado. SERIAL NUMBER GIVEN NAME SURNAME
7 Huella Digital				
7.1 Thumbprint algorithm	SHA1	√	X	
7.2 Thumbprint		√	X	Asignado por la plataforma al momento de generar el certificado

3. CERTIFICADO FUNCION PUBLICA HARDWARE / FIRMA CENTRALIZADA

CERTIFICADO FUNCION PUBLICA HARDWARE / FIRMA CENTRALIZADA				
Campo	**Contenido**	**Obligatorio**	**Crítico**	**Observaciones**
1 TBSCertificate				
1.1 Versión	V3	√	X	[RFC5280]
1.2 Serial number		√	X	Asignado por la plataforma al momento de generar el certificado
1.3 Signature algorithm	Sha256RSA	√	X	OID 1.2.840.113549.1.1.11
1.4 Signature hash algorithm	SHA256	√	X	
2 Issuer				
2.1 Email (E)	ca@gse.co	√	-	
2.2 Common Name (CN)	GSE SUB001_CO	√	X	OID 2.5.4.3
2.3 Organization	GESTION DE SEGURIDAD ELECTRONICA S.A. - GSE	√	-	OID 2.5.4.10
2.4 Serial Number	9002042728	√	-	OID 2.5.4.5
2.5 Organizational Unit	Internet Certification Authority http://www.gse.co	√	-	OID 2.5.4.11
2.6 Title	Subordinate Certificate			OID 2.5.4.12
2.7 StreetAddress	http://www.gse.co/address	√	-	OID 2.5.4.9
2.8 Locality	BOGOTÁ, D.C.	√	-	OID 2.5.4.7
2.9 Country	CO	√	X	OID 2.5.4.6
2.10 Description	GSE Subordinate Certificate 001 Colombia HW-KUSU	√	-	OID 2.5.4.13
3 Validity				
3.1 notBefore		√	X	Asignado por la plataforma al momento de generar el certificado - UTC Time - 5
3.2 notAfter		√	X	Asignado por la plataforma al momento de generar el certificado - UTC Time - 5

4 Subject				
4.1 Description	Certificado de Función Pública - Emitido por GSE SUB001_CO	√	-	OID 2.5.4.13
4.2 Common Name (CN)	Nombre y apellidos del suscriptor	√	-	OID 2.5.4.3 APELLIDO1 APELLIDO2 NOMBRE1 NOMBRE2 (en mayúsculas sin separadores entre los apellidos y los nombres)
4.3 1.3.6.1.4.1.31136.2.2.1.2.1	Tipo de Identificación Personal	√	-	Tipo de Identificación Personal
4.4 Serial Number	Número de documento del suscriptor	√	-	OID 2.5.4.5 Numero de documento
4.5 Email Address	Email del suscriptor	√	-	Email del suscriptor
4.6 Organization	Razón Social de la organización del suscriptor	√	-	OID 2.5.4.10 Nombre o Razón social de la empresa
4.7 1.3.6.1.4.1.31136.2.2.1.2.2	Tipo de Identificación de la Empresa	√	-	Tipo de Identificación de la Empresa
4.8 1.3.6.1.4.1.31136.2.2.1.2.3	Número de Identificación de la Empresa	√	-	Número de Identificación de la Empresa
4.9 1.3.6.1.4.1.31136.2.2.1.2.4	Entidad donde se registra la empresa	√	-	(Opcional) Entidad encargada de registrar la empresa ejemplo Cámara de comercio, superintendencia, etc.
4.10 Title	Cargo del suscriptor en la organización	√	-	OID 2.5.4.12 Cargo del Suscriptor
4.11 Organizational Unit (OU)	Departamento de la organización del suscriptor	√	-	OID 2.5.4.11 Dependencia en la empresa
4.12 1.3.6.1.4.1.31136.2.2.1.2.5	Número Acta de Nombramiento	√	-	Número Acta de Nombramiento
4.13 1.3.6.1.4.1.31136.2.2.1.2.6	Número de Acta de Posesión	√	-	Número de Acta de Posesión
4.14 1.3.6.1.4.1.31136.2.2.1.2.7	Fecha Acta de Posesión	√	-	Fecha Acta de Posesión
4.15 StreetAddress	Dirección de la Organización	√	-	OID 2.5.4.9 Dirección de la empresa

4.16 stateOrProvinceName	Estado / Departamento de la organización del suscriptor	√	-	OID 2.5.4.8 Departamento / Estado de la empresa
4.17 Locality	Municipio / Ciudad de la organización Suscriptor	√	-	OID 2.5.4.7 Municipio / ciudad de la empresa
4.18 Surname	Apellidos del suscriptor	√	-	OID 2.5.4.4 APELLIDO1 APELLIDO2 (en mayúsculas sin separadores entre los apellidos)
4.19 Given Name	Nombre de suscriptor	√	-	OID 2.5.4.42 NOMBRE1 NOMBRE2 (en mayúsculas sin separadores entre los nombres)
4.20 Country	Nacionalidad del Suscriptor	√	-	OID 2.5.4.6 Nacionalidad del Suscriptor; Código de país de dos dígitos según ISO 3166-1.
4.21 Subject Publica Key Info	RSAEncryption Clave Pública de 2048 bits (RF3279) Clave Pública de 2048 bits (RF3279)	√	X	OID 1.2.840.113549.1.1.1 Clave pública de 2048 bits [RFC3279]
4.22 Public key parameters	"0500"	√	X	
5 Extensions				
5.1 Standard Extensions				
5.1.1 Authority Key Identifier	KeyID=8e 4a 03 5e a3 fd 09 a7 63 b5 64 ee 75 46 7a 6c dd be 45 49	√	X	OID 2.5.29.35
5.1.1.1 keyIdentifier		√	-	
5.1.1.2 authorityCertIssuer		√	-	
5.1.1.3 authorityCertSerialNumber		√	-	
5.1.2 Subject Key Identifier		√	-	OID 2.5.29.14
5.1.3 Key Usage		√	-	OID 2.5.29.15
5.1.3.1 digitalSignature	"1"	X	-	

5.1.3.2 nonRepudiation-ContentCommitment	"1"	X	-	
5.1.3.3 keyEncipherment	"1"	X	-	
5.1.3.4 dataEncipherment	"1"	X	-	
5.1.3.5 keyAgreement	"1"	X	-	
5.1.3.6 keyCertSign	"0"	√	-	
5.1.3.7 cRLSign	"0"	√	-	
5.1.3.8 encipherOnly	"0"	X	-	
5.1.3.9 decipherOnly	"0"	X	-	
5.1.4 Certificate Policies		√	X	OID 2.5.29.32
5.1.4.1 Policy Identifier	1.3.6.1.4.1.31136.2.2.3.4.2 - En Token 1.3.6.1.4.1.31136.2.2.3.4.3 - En HSM	√	-	OID Definido por ECD GSE
5.1.4.2 Policy Qualifier ID		√	-	
5.1.4.2.1 CPS Pointer	http://cps.gse.co/sub/cps_sub001_ca_gse.pdf	√	-	OID 1.3.6.1.5.5.7.2.1
5.1.4.2.2 User Notice	Terms of use at CPS CA GSE http://cps.gse.co/sub/cps_sub001_ca_gse.pdf	√	-	
5.1.5 Subject Alternative Name				
5.1.6 Issuer Alternative Name	URI:http://www.gse.co	√	X	OID 2.5.29.18

5.1.7 Subject Directory Attributes	No está presente	X	X	OID 2.5.29.9
5.1.8 Basic Constraints		√	√	
5.1.8.1 cA	End Entity	√	-	
5.1.8.2 pathLenConstraint	No está presente	√	-	
5.1.9 Name Constraints	No está presente	X	X	
5.1.10 Policy Constraints	No está presente	X	X	
5.1.11 Extended Key Usage	No está presente	X	X	OID 2.5.29.37
5.1.11.1 serverAuth	"0"	-	-	OID 1.3.6.1.5.5.7.3.1
5.1.11.2 clientAuth	"1"	-	-	OID 1.3.6.1.5.5.7.3.2
5.1.11.3 codeSigning	"0"	-	-	OID 1.3.6.1.5.5.7.3.3
5.1.11.4 emailProtection	"1"	-	-	OID 1.3.6.1.5.5.7.3.4
5.1.11.5 timeStamping	"0"	-	-	OID 1.3.6.1.5.5.7.3.8
5.1.11.6 OCSPSigning	"0"	-	-	OID 1.3.6.1.5.5.7.3.9
5.1.11.7 Microsoft Smart Card Logon for Windows 1.3.6.2.1.311.20.2.2	"1"	-	-	OID 1.3.6.1.4.1.311.20.2 .2
5.1.11.8 Microsoft Commercial Code Signing 1.3.6.2.1.311.2.1.22	"0"	-	-	OID 1.3.6.1.4.1.311.2.1. 22

5.1.11.9 Microsoft Encrypting File System 1.3.6.2.1.31136.10.3.4	"1"	-	-	OID 1.3.6.1.4.1.311.10.3 .4
5.1.12 CRL Distribution Points		√	-	OID 2.5.29.31
5.1.12.1 CRL Distribution Point 1	URL=http://crl.gse.co/sub/crl_gse_sub001_sha2.crl	√	-	
5.1.12.2 CRL Distribution Point 2	URL=http://crl1.gse.co/sub/crl_gse_sub001_sha2.crl	√	-	
5.1.13 qcStatements	No está presente	-	-	OID 1.3.6.1.5.5.7.1.3
5.1.13.1 id-etsi-qcs-QcCompliance	No está presente	-	-	
5.1.13.2 id-etsi-qcs-QcLimitValue	No está presente	-	-	
5.1.13.3 id-etsi-qcs-QcSSCD	No está presente	-	-	
5.1.14 Netscape Cert Type	No está presente	√	-	
5.1.15 Netscape Revocation URL	No está presente	-	-	
5.1.16 Netscape CA Policy URL	No está presente	-	-	
5.1.17 Netscape Comment	No está presente	-	-	
5.1.18 biometricInfo	No está presente	-	-	
5.1.19 Inhibit Any-Policy	No está presente	-	-	
5.1.20 Freshest CRL	No está presente	-	-	
5.2 Internet Certificate Extensions				

5.2.1 Authority Information Access 1		√	-	OID 1.3.6.1.5.5.7.1.1
5.2.1.1 accessMethod	Certification Authority Issuer (1.3.6.1.5.5.7.48.2)	√	-	
5.2.1.2 accessLocation	URI:http://certs.gse.co/sub/crt_gse_sub001_sha2.crt	√	-	
5.2.2 Authority Information Access 2		-	-	
5.2.2.1 accessMethod	On-line Certificate Status Protocol (1.3.6.1.5.5.7.48.1)	-	-	
5.2.2.2 accessLocation	URI:http://ocsp.gse.co	-	-	
5.2.3 Subject Information Access	No está presente	-	-	
6 PKCS#12				
6.1. Friendly Name		-	-	Asignado por la plataforma al momento de generar el certificado. SERIAL NUMBER GIVEN NAME SURNAME
7 Huella Digital				
7.1 Thumbprint algorithm	SHA1	√	X	
7.2 Thumbprint		√	X	Asignado por la plataforma al momento de generar el certificado

4. CERTIFICADO DE PROFESIONAL TITULADO HARDWARE / FIRMA CENTRALIZADA

CERTIFICADO DE PROFESIONAL TITULADO HARDWARE / FIRMA CENTRALIZADA				
Campo	**Contenido**	**Obligatorio**	**Crítico**	**Observaciones**

GESTIÓN DE SEGURIDAD ELECTRÓNICA	**Anexo 1** **Perfil técnico certificados digitales GSE SUB001_CO**	Fecha de vigencia	27/11/2018
		Versión	3

1 TBSCertificate				
1.1 Versión	V3	√	X	[RFC5280]
1.2 Serial number		√	X	Asignado por la plataforma al momento de generar el certificado
1.3 Signature algorithm	Sha256RSA	√	X	OID 1.2.840.113549.1.1.11
1.4 Signature hash algorithm	SHA256	√	X	
2 Issuer				
2.1 Email (E)	ca@gse.co	√	-	
2.2 Common Name (CN)	GSE SUB001_CO	√	X	OID 2.5.4.3
2.3 Organization	GESTION DE SEGURIDAD ELECTRONICA S.A. - GSE	√	-	OID 2.5.4.10
2.4 Serial Number	9002042728	√	-	OID 2.5.4.5
2.5 Organizational Unit	Internet Certification Authority http://www.gse.co	√	-	OID 2.5.4.11
2.6 Title	Subordinate Certificate			OID 2.5.4.12
2.7 StreetAddress	http://www.gse.co/address	√	-	OID 2.5.4.9
2.8 Locality	BOGOTÁ, D.C.	√	-	OID 2.5.4.7
2.9 Country	CO	√	X	OID 2.5.4.6
2.10 Description	GSE Subordinate Certificate 001 Colombia HW-KUSU	√	-	OID 2.5.4.13
3 Validity				
3.1 notBefore		√	X	Asignado por la plataforma al momento de generar el certificado - UTC Time - 5
3.2 notAfter		√	X	Asignado por la plataforma al momento de generar el certificado - UTC Time - 5
4 Subject				

4.1 Description	Certificado de Profesional Titulado - Emitido por GSE SUB001_CO	√	-	OID 2.5.4.13
4.2 Common Name (CN)	Nombre y apellidos del suscriptor	√	-	OID 2.5.4.3 APELLIDO1 APELLIDO2 NOMBRE1 NOMBRE2 (en mayúsculas sin separadores entre los apellidos y los nombres)
4.3 1.3.6.1.4.1.31136.2.2.1.2.1	Tipo de Identificación Personal	√	-	Tipo de Identificación Personal
4.4 Serial Number	Número de documento del suscriptor	√	-	OID 2.5.4.5 Numero de documento
4.5 Email Address	Email del suscriptor	√	-	Email del suscriptor
4.7 1.3.6.1.4.1.31136.2.2.1.2.8	Numero Matricula Profesional	√	-	Numero Matricula Profesional
4.8 1.3.6.1.4.1.31136.2.2.1.2.9	Fecha Matricula Profesional	√	-	Fecha Matricula Profesional
4.9 1.3.6.1.4.1.31136.2.2.1.2.10	Entidad que emite su tarjeta o matricula profesional y/o técnica	√	-	Institución donde se registra la profesión
4.10 Title	Nombre del Titulo Profesional	√	-	OID 2.5.4.12 Nombre del Titulo Profesional
4.11 Organizational Unit (OU)	Universidad otorgante del titulo	√	-	OID 2.5.4.11 Universidad otorgante del titulo
4.12 StreetAddress	Dirección del suscriptor	√	-	OID 2.5.4.9 Dirección de la empresa
4.13 StateOrProvinceName	Estado / Departamento del suscriptor	√	-	OID 2.5.4.8 Departamento / Estado de la empresa
4.14 Locality	Municipio / Ciudad del Suscriptor	√	-	OID 2.5.4.7 Municipio / ciudad de la empresa
4.15 Surname	Apellidos del suscriptor	√	-	OID 2.5.4.4 APELLIDO1 APELLIDO2 (en mayúsculas sin separadores entre los apellidos)
4.16 Given Name	Nombre de suscriptor	√	-	OID 2.5.4.42 NOMBRE1 NOMBRE2 (en mayúsculas sin separadores entre los nombres)
4.17 Country	Nacionalidad del Suscriptor	√	-	OID 2.5.4.6 Nacionalidad del Suscriptor; Código de país de dos dígitos según ISO 3166-1.

4.18 Subject Publica Key Info	RSAEncryption Clave Pública de 2048 bits (RF3279) Clave Pública de 2048 bits (RF3279)	√	X	OID 1.2.840.113549.1.1.1 Clave pública de 2048 bits [RFC3279]
4.19 Public key parameters	"0500"	√	X	
5 Extensions				
5.1 Standard Extensions				
5.1.1 Authority Key Identifier	KeyID=8e 4a 03 5e a3 fd 09 a7 63 b5 64 ee 75 46 7a 6c dd be 45 49	√	X	OID 2.5.29.35
5.1.1.1 keyIdentifier		√	-	
5.1.1.2 authorityCertIssuer		√	-	
5.1.1.3 authorityCertSerialNumber		√	-	
5.1.2 Subject Key Identifier		√	-	OID 2.5.29.14
5.1.3 Key Usage		√	-	OID 2.5.29.15
5.1.3.1 digitalSignature	"1"	X	-	
5.1.3.2 nonRepudiation-ContentCommitment	"1"	X	-	
5.1.3.3 keyEncipherment	"1"	X	-	
5.1.3.4 dataEncipherment	"1"	X	-	
5.1.3.5 keyAgreement	"1"	X	-	
5.1.3.6 keyCertSign	"0"	√	-	

5.1.3.7 cRLSign	"0"	√	-	
5.1.3.8 encipherOnly	"0"	X	-	
5.1.3.9 decipherOnly	"0"	X	-	
5.1.4 Certificate Policies		√	X	OID 2.5.29.32
5.1.4.1 Policy Identifier	1.3.6.1.4.1.31136.2.2.3.6.2 - En token 1.3.6.1.4.1.31136.2.2.3.6.3 - En HSM	√	-	OID Definido por ECD GSE
5.1.4.2 Policy Qualifier ID		√	-	
5.1.4.2.1 CPS Pointer	http://cps.gse.co/sub/cps_sub001_ca_gse.pdf	√	-	OID 1.3.6.1.5.5.7.2.1
5.1.4.2.2 User Notice	Terms of use at CPS CA GSE http://cps.gse.co/sub/cps_sub001_ca_gse.pdf	√	-	
5.1.5 Subject Alternative Name				
5.1.6 Issuer Alternative Name	URI:http://www.gse.co	√	X	OID 2.5.29.18
5.1.7 Subject Directory Attributes	No está presente	X	X	OID 2.5.29.9
5.1.8 Basic Constraints		√	√	
5.1.8.1 cA	End Entity	√	-	
5.1.8.2 pathLenConstraint	No está presente	√	-	
5.1.9 Name Constraints	No está presente	X	X	

5.1.10 Policy Constraints	No está presente	X	X	
5.1.11 Extended Key Usage	No está presente	X	X	OID 2.5.29.37
5.1.11.1 serverAuth	"0"	-	-	OID 1.3.6.1.5.5.7.3.1
5.1.11.2 clientAuth	"1"	-	-	OID 1.3.6.1.5.5.7.3.2
5.1.11.3 codeSigning	"0"	-	-	OID 1.3.6.1.5.5.7.3.3
5.1.11.4 emailProtection	"1"	-	-	OID 1.3.6.1.5.5.7.3.4
5.1.11.5 timeStamping	"0"	-	-	OID 1.3.6.1.5.5.7.3.8
5.1.11.6 OCSPSigning	"0"	-	-	OID 1.3.6.1.5.5.7.3.9
5.1.11.7 Microsoft Smart Card Logon for Windows 1.3.6.2.1.311.20.2.2	"1"	-	-	OID 1.3.6.1.4.1.311.20.2 .2
5.1.11.8 Microsoft Commercial Code Signing 1.3.6.2.1.311.2.1.22	"0"	-	-	OID 1.3.6.1.4.1.311.2.1. 22
5.1.11.9 Microsoft Encrypting File System 1.3.6.2.1.31136.10.3.4	"1"	-	-	OID 1.3.6.1.4.1.311.10.3 .4
5.1.12 CRL Distribution Points		√	-	OID 2.5.29.31
5.1.12.1 CRL Distribution Point 1	URL=http://crl.gse.co/sub/crl_gse_sub001_sha2.crl	√	-	

5.1.12.2 CRL Distribution Point 2	URL=http://crl1.gse.co/sub/crl_gse_sub001_sha2.crl	√	-	
5.1.13 qcStatements	No está presente	-	-	OID 1.3.6.1.5.5.7.1.3
5.1.13.1 id-etsi-qcs-QcCompliance	No está presente	-	-	
5.1.13.2 id-etsi-qcs-QcLimitValue	No está presente	-	-	
5.1.13.3 id-etsi-qcs-QcSSCD	No está presente	-	-	
5.1.14 Netscape Cert Type	No está presente	√	-	
5.1.15 Netscape Revocation URL	No está presente	-	-	
5.1.16 Netscape CA Policy URL	No está presente	-	-	
5.1.17 Netscape Comment	No está presente	-	-	
5.1.18 biometricInfo	No está presente	-	-	
5.1.19 Inhibit Any-Policy	No está presente	-	-	
5.1.20 Freshest CRL	No está presente	-	-	
5.2 Internet Certificate Extensions				
5.2.1 Authority Information Access 1		√	-	OID 1.3.6.1.5.5.7.1.1
5.2.1.1 accessMethod	Certification Authority Issuer (1.3.6.1.5.5.7.48.2)	√	-	
5.2.1.2 accessLocation	URI:http://certs.gse.co/sub/crt_gse_sub001_sha2.crt	√	-	

5.2.2 Authority Information Access 2		-	-	
5.2.2.1 accessMethod	On-line Certificate Status Protocol (1.3.6.1.5.5.7.48.1)	-	-	
5.2.2.2 accessLocation	URI:http://ocsp.gse.co	-	-	
5.2.3 Subject Information Access	No está presente	-	-	
6 PKCS#12				
6.1. Friendly Name		-	-	Asignado por la plataforma al momento de generar el certificado. SERIAL NUMBER GIVEN NAME SURNAME
7 Huella Digital				
7.1 Thumbprint algorithm	SHA1	√	X	
7.2 Thumbprint		√	X	Asignado por la plataforma al momento de generar el certificado

5. CERTIFICADO DE TECNICO PROFESIONAL HARDWARE / FIRMA CENTRALIZADA

CERTIFICADO DE TECNICO PROFESIONAL HARDWARE / FIRMA CENTRALIZADA				
Campo	**Contenido**	**Obligatorio**	**Crítico**	**Observaciones**
1 TBSCertificate				
1.1 Versión	V3	√	X	[RFC5280]
1.2 Serial number		√	X	Asignado por la plataforma al momento de generar el certificado
1.3 Signature algorithm	Sha256RSA	√	X	OID 1.2.840.113549.1.1.11

1.4 Signature hash algorithm	SHA256	√	X	
2 Issuer				
2.1 Email (E)	ca@gse.co	√	-	
2.2 Common Name (CN)	GSE SUB001_CO	√	X	OID 2.5.4.3
2.3 Organization	GESTION DE SEGURIDAD ELECTRONICA S.A. - GSE	√	-	OID 2.5.4.10
2.4 Serial Number	9002042728	√	-	OID 2.5.4.5
2.5 Organizational Unit	Internet Certification Authority http://www.gse.co	√	-	OID 2.5.4.11
2.6 Title	Subordinate Certificate			OID 2.5.4.12
2.7 StreetAddress	http://www.gse.co/address	√	-	OID 2.5.4.9
2.8 Locality	BOGOTÁ, D.C.	√	-	OID 2.5.4.7
2.9 Country	CO	√	X	OID 2.5.4.6
2.10 Description	GSE Subordinate Certificate 001 Colombia HW-KUSU	√	-	OID 2.5.4.13
3 Validity				
3.1 notBefore		√	X	Asignado por la plataforma al momento de generar el certificado - UTC Time - 5
3.2 notAfter		√	X	Asignado por la plataforma al momento de generar el certificado - UTC Time - 5
4 Subject				
4.1 Description	Certificado de Técnico Profesional - Emitido por GSE SUB001_CO	√	-	OID 2.5.4.13
4.2 Common Name (CN)	Nombre y apellidos del suscriptor	√	-	OID 2.5.4.3 APELLIDO1 APELLIDO2 NOMBRE1 NOMBRE2 (en mayúsculas sin separadores entre los apellidos y los nombres)

4.3 1.3.6.1.4.1.31136.2.2.1.2.1	Tipo de Identificación Personal	√	-	Tipo de Identificación Personal
4.4 Serial Number	Número de documento del suscriptor	√	-	OID 2.5.4.5 Numero de documento
4.5 Email Address	Email del suscriptor	√	-	Email del suscriptor
4.7 1.3.6.1.4.1.31136.2.2.1.2.8	Numero Matricula Tecnica	√	-	Numero Matricula Profesional
4.8 1.3.6.1.4.1.31136.2.2.1.2.9	Fecha Matricula Tecnica	√	-	Fecha Matricula Profesional
4.9 1.3.6.1.4.1.31136.2.2.1.2.10	Entidad que emite su tarjeta o matricula profesional y/o técnica	√	-	Institución donde se registra la profesión
4.10 Title	Nombre del Titulo Tecnica	√	-	OID 2.5.4.12 Nombre del Titulo Profesional
4.11 Organizational Unit (OU)	Universidad y/o Institución otorgante del titulo	√	-	OID 2.5.4.11 Universidad otorgante del titulo
4.12 StreetAddress	Dirección del suscriptor	√	-	OID 2.5.4.9 Dirección de la empresa
4.13 StateOrProvinceName	Estado / Departamento del suscriptor	√	-	OID 2.5.4.8 Departamento / Estado de la empresa
4.14 Locality	Municipio / Ciudad del Suscriptor	√	-	OID 2.5.4.7 Municipio / ciudad de la empresa
4.15 Surname	Apellidos del suscriptor	√	-	OID 2.5.4.4 APELLIDO1 APELLIDO2 (en mayúsculas sin separadores entre los apellidos)
4.16 Given Name	Nombre de suscriptor	√	-	OID 2.5.4.42 NOMBRE1 NOMBRE2 (en mayúsculas sin separadores entre los nombres)
4.17 Country	Nacionalidad del Suscriptor	√	-	OID 2.5.4.6 Nacionalidad del Suscriptor; Código de país de dos dígitos según ISO 3166-1.
4.18 Subject Publica Key Info	RSAEncryption Clave Pública de 2048 bits (RF3279) Clave Pública de 2048 bits (RF3279)	√	X	OID 1.2.840.113549.1.1.1 Clave pública de 2048 bits [RFC3279]
4.19 Public key parameters	"0500"	√	X	
5 Extensions				

5.1 Standard Extensions				
5.1.1 Authority Key Identifier	KeyID=8e 4a 03 5e a3 fd 09 a7 63 b5 64 ee 75 46 7a 6c dd be 45 49	√	X	OID 2.5.29.35
5.1.1.1 keyIdentifier		√	-	
5.1.1.2 authorityCertIssuer		√	-	
5.1.1.3 authorityCertSerialNumber		√	-	
5.1.2 Subject Key Identifier		√	-	OID 2.5.29.14
5.1.3 Key Usage		√	-	OID 2.5.29.15
5.1.3.1 digitalSignature	"1"	X	-	
5.1.3.2 nonRepudiation-ContentCommitment	"1"	X	-	
5.1.3.3 keyEncipherment	"1"	X	-	
5.1.3.4 dataEncipherment	"1"	X	-	
5.1.3.5 keyAgreement	"1"	X	-	
5.1.3.6 keyCertSign	"0"	√	-	
5.1.3.7 cRLSign	"0"	√	-	
5.1.3.8 encipherOnly	"0"	X	-	
5.1.3.9 decipherOnly	"0"	X	-	

5.1.4 Certificate Policies		√	X	OID 2.5.29.32
5.1.4.1 Policy Identifier	1.3.6.1.4.1.31136.2.2.3.7.2 - En token 1.3.6.1.4.1.31136.2.2.3.7.3 - En HSM	√	-	OID Definido por ECD GSE
5.1.4.2 Policy Qualifier ID		√	-	
5.1.4.2.1 CPS Pointer	http://cps.gse.co/sub/cps_sub001_ca_gse.pdf	√	-	OID 1.3.6.1.5.5.7.2.1
5.1.4.2.2 User Notice	Terms of use at CPS CA GSE http://cps.gse.co/sub/cps_sub001_ca_gse.pdf	√	-	
5.1.5 Subject Alternative Name				
5.1.6 Issuer Alternative Name	URI:http://www.gse.co	√	X	OID 2.5.29.18
5.1.7 Subject Directory Attributes	No está presente	X	X	OID 2.5.29.9
5.1.8 Basic Constraints		√	√	
5.1.8.1 cA	End Entity	√	-	
5.1.8.2 pathLenConstraint	No está presente	√	-	
5.1.9 Name Constraints	No está presente	X	X	
5.1.10 Policy Constraints	No está presente	X	X	
5.1.11 Extended Key Usage	No está presente	X	X	OID 2.5.29.37
5.1.11.1 serverAuth	"0"	-	-	OID 1.3.6.1.5.5.7.3.1
5.1.11.2 clientAuth	"1"	-	-	OID 1.3.6.1.5.5.7.3.2

5.1.11.3 codeSigning	"0"	-	-	OID 1.3.6.1.5.5.7.3.3
5.1.11.4 emailProtection	"1"	-	-	OID 1.3.6.1.5.5.7.3.4
5.1.11.5 timeStamping	"0"	-	-	OID 1.3.6.1.5.5.7.3.8
5.1.11.6 OCSPSigning	"0"	-	-	OID 1.3.6.1.5.5.7.3.9
5.1.11.7 Microsoft Smart Card Logon for Windows 1.3.6.2.1.311.20.2.2	"1"	-	-	OID 1.3.6.1.4.1.311.20.2 .2
5.1.11.8 Microsoft Commercial Code Signing 1.3.6.2.1.311.2.1.22	"0"	-	-	OID 1.3.6.1.4.1.311.2.1. 22
5.1.11.9 Microsoft Encrypting File System 1.3.6.2.1.31136.10.3.4	"1"	-	-	OID 1.3.6.1.4.1.311.10.3 .4
5.1.12 CRL Distribution Points		√	-	OID 2.5.29.31
5.1.12.1 CRL Distribution Point 1	URL=http://crl.gse.co/sub/crl_gse_sub001_sha2.crl	√	-	
5.1.12.2 CRL Distribution Point 2	URL=http://crl1.gse.co/sub/crl_gse_sub001_sha2.crl	√	-	
5.1.13 qcStatements	No está presente	-	-	OID 1.3.6.1.5.5.7.1.3
5.1.13.1 id-etsi-qcs-QcCompliance	No está presente	-	-	
5.1.13.2 id-etsi-qcs-QcLimitValue	No está presente	-	-	

5.1.13.3 id-etsi-qcs-QcSSCD	No está presente	-	-	
5.1.14 Netscape Cert Type	No está presente	√	-	
5.1.15 Netscape Revocation URL	No está presente	-	-	
5.1.16 Netscape CA Policy URL	No está presente	-	-	
5.1.17 Netscape Comment	No está presente	-	-	
5.1.18 biometricInfo	No está presente	-	-	
5.1.19 Inhibit Any-Policy	No está presente	-	-	
5.1.20 Freshest CRL	No está presente	-	-	
5.2 Internet Certificate Extensions				
5.2.1 Authority Information Access 1		√	-	OID 1.3.6.1.5.5.7.1.1
5.2.1.1 accessMethod	Certification Authority Issuer (1.3.6.1.5.5.7.48.2)	√	-	
5.2.1.2 accessLocation	URI:http://certs.gse.co/sub/crt_gse_sub001_sha2.crt	√	-	
5.2.2 Authority Information Access 2		-	-	
5.2.2.1 accessMethod	On-line Certificate Status Protocol (1.3.6.1.5.5.7.48.1)	-	-	
5.2.2.2 accessLocation	URI:http://ocsp.gse.co	-	-	
5.2.3 Subject Information Access	No está presente	-	-	

6 PKCS#12				
6.1. Friendly Name		-	-	Asignado por la plataforma al momento de generar el certificado. SERIAL NUMBER GIVEN NAME SURNAME
7 Huella Digital				
7.1 Thumbprint algorithm	SHA1	√	X	
7.2 Thumbprint		√	X	Asignado por la plataforma al momento de generar el certificado

6. CERTIFICADO DE PERSONA NATURAL HARDWARE / FIRMA CENTRALIZADA

CERTIFICADO DE PERSONA NATURAL HARDWARE / FIRMA CENTRALIZADA				
Campo	**Contenido**	**Obligatorio**	**Crítico**	**Observaciones**
1 TBSCertificate				
1.1 Versión	V3	√	X	[RFC5280]
1.2 Serial number		√	X	Asignado por la plataforma al momento de generar el certificado
1.3 Signature algorithm	Sha256RSA	√	X	OID 1.2.840.113549.1.1.11
1.4 Signature hash algorithm	SHA256	√	X	
2 Issuer				
2.1 Email (E)	ca@gse.co	√	-	

2.2 Common Name (CN)	GSE SUB001_CO	√	X	OID 2.5.4.3
2.3 Organization	GESTION DE SEGURIDAD ELECTRONICA S.A. - GSE	√	-	OID 2.5.4.10
2.4 Serial Number	9002042728	√	-	OID 2.5.4.5
2.5 Organizational Unit	Internet Certification Authority http://www.gse.co	√	-	OID 2.5.4.11
2.6 Title	Subordinate Certificate			OID 2.5.4.12
2.7 StreetAddress	http://www.gse.co/address	√	-	OID 2.5.4.9
2.8 Locality	BOGOTÁ, D.C.	√	-	OID 2.5.4.7
2.9 Country	CO	√	X	OID 2.5.4.6
2.10 Description	GSE Subordinate Certificate 001 Colombia HW-KUSU	√	-	OID 2.5.4.13
3 Validity				
3.1 notBefore		√	X	Asignado por la plataforma al momento de generar el certificado - UTC Time - 5
3.2 notAfter		√	X	Asignado por la plataforma al momento de generar el certificado - UTC Time - 5
4 Subject				
4.1 Description	Certificado de Persona Natural - Emitido por GSE SUB001_CO	√	-	OID 2.5.4.13
4.2 Common Name (CN)	Nombre y apellidos del suscriptor	√	-	OID 2.5.4.3 APELLIDO1 APELLIDO2 NOMBRE1 NOMBRE2 (en mayúsculas sin separadores entre los apellidos y los nombres)
4.3 1.3.6.1.4.1.31136.2.2.1.2.1	Tipo de Identificación Personal	√	-	Tipo de Identificación Personal
4.4 Serial Number	Número de documento del suscriptor	√	-	OID 2.5.4.5 Numero de documento
4.5 Email Address	Email del suscriptor	√	-	Email del suscriptor
4.12 StreetAddress	Dirección del Suscriptor	√	-	OID 2.5.4.9 Dirección de la empresa

4.13 StateOrProvinceName	Estado / Departamento del Suscriptor	√	-	OID 2.5.4.8 Departamento / Estado de la empresa
4.14 Locality	Municipio / Ciudad del Suscriptor	√	-	OID 2.5.4.7 Municipio / ciudad de la empresa
4.15 Surname	Apellidos del suscriptor	√	-	OID 2.5.4.4 APELLIDO1 APELLIDO2 (en mayúsculas sin separadores entre los apellidos)
4.16 Given Name	Nombre de suscriptor	√	-	OID 2.5.4.42 NOMBRE1 NOMBRE2 (en mayúsculas sin separadores entre los nombres)
4.17 Country	Nacionalidad del Suscriptor	√	-	OID 2.5.4.6 Nacionalidad del Suscriptor; Código de país de dos dígitos según ISO 3166-1.
4.18 Subject Publica Key Info	RSAEncryption Clave Pública de 2048 bits (RF3279) Clave Pública de 2048 bits (RF3279)	√	X	OID 1.2.840.113549.1.1.1 Clave pública de 2048 bits [RFC3279]
4.19 Public key parameters	"0500"	√	X	
5 Extensions				
5.1 Standard Extensions				
5.1.1 Authority Key Identifier	KeyID=8e 4a 03 5e a3 fd 09 a7 63 b5 64 ee 75 46 7a 6c dd be 45 49	√	X	OID 2.5.29.35
5.1.1.1 keyIdentifier		√	-	
5.1.1.2 authorityCertIssuer		√	-	
5.1.1.3 authorityCertSerialNumber		√	-	
5.1.2 Subject Key Identifier		√	-	OID 2.5.29.14
5.1.3 Key Usage		√	-	OID 2.5.29.15
5.1.3.1 digitalSignature	"1"	X	-	

5.1.3.2 nonRepudiation-ContentCommitment	"1"	X	-	
5.1.3.3 keyEncipherment	"1"	X	-	
5.1.3.4 dataEncipherment	"1"	X	-	
5.1.3.5 keyAgreement	"1"	X	-	
5.1.3.6 keyCertSign	"0"	√	-	
5.1.3.7 cRLSign	"0"	√	-	
5.1.3.8 encipherOnly	"0"	X	-	
5.1.3.9 decipherOnly	"0"	X	-	
5.1.4 Certificate Policies		√	X	OID 2.5.29.32
5.1.4.1 Policy Identifier	1.3.6.1.4.1.31136.2.2.3.9.2 - En token 1.3.6.1.4.1.31136.2.2.3.9.3 - En HSM	√	-	OID Definido por ECD GSE
5.1.4.2 Policy Qualifier ID		√	-	
5.1.4.2.1 CPS Pointer	http://cps.gse.co/sub/cps_sub001_ca_gse.pdf	√	-	OID 1.3.6.1.5.5.7.2.1
5.1.4.2.2 User Notice	Terms of use at CPS CA GSE http://cps.gse.co/sub/cps_sub001_ca_gse.pdf	√	-	
5.1.5 Subject Alternative Name				
5.1.6 Issuer Alternative Name	URI:http://www.gse.co	√	X	OID 2.5.29.18

5.1.7 Subject Directory Attributes	No está presente	X	X	OID 2.5.29.9
5.1.8 Basic Constraints		√	√	
5.1.8.1 cA	End Entity	√	-	
5.1.8.2 pathLenConstraint	No está presente	√	-	
5.1.9 Name Constraints	No está presente	X	X	
5.1.10 Policy Constraints	No está presente	X	X	
5.1.11 Extended Key Usage	No está presente	X	X	OID 2.5.29.37
5.1.11.1 serverAuth	"0"	-	-	OID 1.3.6.1.5.5.7.3.1
5.1.11.2 clientAuth	"1"	-	-	OID 1.3.6.1.5.5.7.3.2
5.1.11.3 codeSigning	"0"	-	-	OID 1.3.6.1.5.5.7.3.3
5.1.11.4 emailProtection	"1"	-	-	OID 1.3.6.1.5.5.7.3.4
5.1.11.5 timeStamping	"0"	-	-	OID 1.3.6.1.5.5.7.3.8
5.1.11.6 OCSPSigning	"0"	-	-	OID 1.3.6.1.5.5.7.3.9
5.1.11.7 Microsoft Smart Card Logon for Windows 1.3.6.2.1.311.20.2.2	"1"	-	-	OID 1.3.6.1.4.1.311.20.2 .2

5.1.11.8 Microsoft Commercial Code Signing 1.3.6.2.1.311.2.1.22	"0"	-	-	OID 1.3.6.1.4.1.311.2.1. 22
5.1.11.9 Microsoft Encrypting File System 1.3.6.2.1.31136.10.3.4	"1"	-	-	OID 1.3.6.1.4.1.311.10.3 .4
5.1.12 CRL Distribution Points		√	-	OID 2.5.29.31
5.1.12.1 CRL Distribution Point 1	URL=http://crl.gse.co/sub/crl_gse_sub001_sha2.crl	√	-	
5.1.12.2 CRL Distribution Point 2	URL=http://crl1.gse.co/sub/crl_gse_sub001_sha2.crl	√	-	
5.1.13 qcStatements	No está presente	-	-	OID 1.3.6.1.5.5.7.1.3
5.1.13.1 id-etsi-qcs-QcCompliance	No está presente	-	-	
5.1.13.2 id-etsi-qcs-QcLimitValue	No está presente	-	-	
5.1.13.3 id-etsi-qcs-QcSSCD	No está presente	-	-	
5.1.14 Netscape Cert Type	No está presente	√	-	
5.1.15 Netscape Revocation URL	No está presente	-	-	
5.1.16 Netscape CA Policy URL	No está presente	-	-	
5.1.17 Netscape Comment	No está presente	-	-	
5.1.18 biometricInfo	No está presente	-	-	

5.1.19 Inhibit Any-Policy	No está presente	-	-	
5.1.20 Freshest CRL	No está presente	-	-	
5.2 Internet Certificate Extensions				
5.2.1 Authority Information Access 1		√	-	OID 1.3.6.1.5.5.7.1.1
5.2.1.1 accessMethod	Certification Authority Issuer (1.3.6.1.5.5.7.48.2)	√	-	
5.2.1.2 accessLocation	URI:http://certs.gse.co/sub/crt_gse_sub001_sha2.crt	√	-	
5.2.2 Authority Information Access 2		-	-	
5.2.2.1 accessMethod	On-line Certificate Status Protocol (1.3.6.1.5.5.7.48.1)	-	-	
5.2.2.2 accessLocation	URI:http://ocsp.gse.co	-	-	
5.2.3 Subject Information Access	No está presente	-	-	
6 PKCS#12				
6.1. Friendly Name		-	-	Asignado por la plataforma al momento de generar el certificado. SERIAL NUMBER GIVEN NAME SURNAME
7 Huella Digital				
7.1 Thumbprint algorithm	SHA1	√	X	
7.2 Thumbprint		√	X	Asignado por la plataforma al momento de generar el certificado

7. CERTIFICADO DE FACTURA ELECTRONICA

CERTIFICADO DE FACTURA ELECTRONICA HARDWARE / FIRMA CENTRALIZADA				
Campo	**Contenido**	**Obligatorio**	**Crítico**	**Observaciones**
1 TBSCertificate				
1.1 Versión	V3	√	X	[RFC5280]
1.2 Serial number		√	X	Asignado por la plataforma al momento de generar el certificado
1.3 Signature algorithm	Sha256RSA	√	X	OID 1.2.840.113549.1.1.11
1.4 Signature hash algorithm	SHA256	√	X	
2 Issuer				
2.1 Email (E)	ca@gse.co	√	-	
2.2 Common Name (CN)	GSE SUB001_CO	√	X	OID 2.5.4.3
2.3 Organization	GESTION DE SEGURIDAD ELECTRONICA S.A. - GSE	√	-	OID 2.5.4.10
2.4 Serial Number	9002042728	√	-	OID 2.5.4.5
2.5 Organizational Unit	Internet Certification Authority http://www.gse.co	√	-	OID 2.5.4.11
2.6 Title	Subordinate Certificate			OID 2.5.4.12
2.7 StreetAddress	http://www.gse.co/address	√	-	OID 2.5.4.9
2.8 Locality	BOGOTÁ, D.C.	√	-	OID 2.5.4.7
2.9 Country	CO	√	X	OID 2.5.4.6
2.10 Description	GSE Subordinate Certificate 001 Colombia HW-KUSU	√	-	OID 2.5.4.13
3 Validity				

3.1 notBefore		√	X	Asignado por la plataforma al momento de generar el certificado - UTC Time - 5
3.2 notAfter		√	X	Asignado por la plataforma al momento de generar el certificado - UTC Time - 5
4 Subject				
4.1 Description	Certificado de Factura Electrónica - Emitido por GSE SUB001_CO	√	-	OID 2.5.4.13
4.2 Common Name (CN)	Razón Social de la organización	√	-	OID 2.5.4.3 Razón Social de la organización
4.3 1.3.6.1.4.1.31136.2.2.1.2.2	Tipo de Identificación de la Empresa	√	-	Tipo de Identificación de la Empresa
4.4 Serial Number	Número de Identificación de la Empresa	√	-	OID 2.5.4.5 Número de Identificación de la Empresa
4.5 1.3.6.1.4.1.31136.2.2.1.2.4	Entidad donde se registra la empresa	√	-	(Opcional) Entidad encargada de registrar la empresa ejemplo Cámara de comercio, superintendencia, etc.
4.6 1.3.6.1.4.1.31136.2.2.1.2.11	Numero Autorización Factura Electrónica	√	-	Numero Autorización Factura Electrónica
4.7 Email Address	Email empresa facturación	√	-	Email empresa facturación
4.8 Locality	Municipio / Ciudad de la organización Suscriptor	√	-	OID 2.5.4.7 Municipio / ciudad de la empresa
4.9 StreetAddress	Dirección de la Organización	√	-	OID 2.5.4.9 Dirección de la empresa
4.10 Country	Nacionalidad del Suscriptor	√	-	OID 2.5.4.6 Nacionalidad de la empresa; Código de país de dos dígitos según ISO 3166-1.
4.11 StateOrProvinceName	Estado / Departamento de la organización del suscriptor	√	-	OID 2.5.4.8 Departamento / Estado de la empresa
4.12 Organization	Operado por Razón Social de la empresa encarga **(Si aplica)**	√	-	OID 2.5.4.10 Nombre o Razón social de la empresa encarga **(Si aplica)**

4.13 Given Name	Nombre del responsable de facturación **(Si aplica)**	√	-	OID 2.5.4.42 NOMBRE1 NOMBRE2 (en mayúsculas sin separadores entre los nombres) del responsable de facturación **(Si aplica)**
4.14 Surname	Apellidos del responsable de facturación **(Si aplica)**	√	-	OID 2.5.4.4 APELLIDO1 APELLIDO2 (en mayúsculas sin separadores entre los apellidos) del responsable de facturación **(Si aplica)**
4.15 Title	Cargo del suscriptor en la organización **(Si aplica)**	√	-	OID 2.5.4.12 Cargo del responsable en la organización **(Si aplica)**
4.16 Subject Publica Key Info	RSAEncryption Clave Pública de 2048 bits (RF3279) Clave Pública de 2048 bits (RF3279)	√	X	OID 1.2.840.113549.1.1.1 Clave pública de 2048 bits [RFC3279]
4.17 Public key parameters	"0500"	√	X	
5 Extensions				
5.1 Standard Extensions				
5.1.1 Authority Key Identifier	KeyID=8e 4a 03 5e a3 fd 09 a7 63 b5 64 ee 75 46 7a 6c dd be 45 49	√	X	OID 2.5.29.35
5.1.1.1 keyIdentifier		√	-	
5.1.1.2 authorityCertIssuer		√	-	
5.1.1.3 authorityCertSerialNumber		√	-	
5.1.2 Subject Key Identifier		√	-	OID 2.5.29.14
5.1.3 Key Usage		√	-	OID 2.5.29.15
5.1.3.1 digitalSignature	"1"	X	-	

5.1.3.2 nonRepudiation-ContentCommitment	"1"	X	-	
5.1.3.3 keyEncipherment	"1"	X	-	
5.1.3.4 dataEncipherment	"1"	X	-	
5.1.3.5 keyAgreement	"1"	X	-	
5.1.3.6 keyCertSign	"0"	√	-	
5.1.3.7 cRLSign	"0"	√	-	
5.1.3.8 encipherOnly	"0"	X	-	
5.1.3.9 decipherOnly	"0"	X	-	
5.1.4 Certificate Policies		√	X	OID 2.5.29.32
5.1.4.1 Policy Identifier	1.3.6.1.4.1.31136.2.2.3.11.2 - En token 1.3.6.1.4.1.31136.2.2.3.11.3 - En HSM	√	-	OID Definido por ECD GSE
5.1.4.2 Policy Qualifier ID		√	-	
5.1.4.2.1 CPS Pointer	http://cps.gse.co/sub/cps_sub001_ca_gse.pdf	√	-	OID 1.3.6.1.5.5.7.2.1
5.1.4.2.2 User Notice	Terms of use at CPS CA GSE http://cps.gse.co/sub/cps_sub001_ca_gse.pdf	√	-	
5.1.5 Subject Alternative Name				
5.1.6 Issuer Alternative Name	URI:http://www.gse.co	√	X	OID 2.5.29.18

5.1.7 Subject Directory Attributes	No está presente	X	X	OID 2.5.29.9
5.1.8 Basic Constraints		√	√	
5.1.8.1 cA	End Entity	√	-	
5.1.8.2 pathLenConstraint	No está presente	√	-	
5.1.9 Name Constraints	No está presente	X	X	
5.1.10 Policy Constraints	No está presente	X	X	
5.1.11 Extended Key Usage	No está presente	X	X	OID 2.5.29.37
5.1.11.1 serverAuth	"0"	-	-	OID 1.3.6.1.5.5.7.3.1
5.1.11.2 clientAuth	"1"	-	-	OID 1.3.6.1.5.5.7.3.2
5.1.11.3 codeSigning	"0"	-	-	OID 1.3.6.1.5.5.7.3.3
5.1.11.4 emailProtection	"1"	-	-	OID 1.3.6.1.5.5.7.3.4
5.1.11.5 timeStamping	"0"	-	-	OID 1.3.6.1.5.5.7.3.8
5.1.11.6 OCSPSigning	"0"	-	-	OID 1.3.6.1.5.5.7.3.9
5.1.11.7 Microsoft Smart Card Logon for Windows 1.3.6.2.1.311.20.2.2	"1"	-	-	OID 1.3.6.1.4.1.311.20.2 .2

5.1.11.8 Microsoft Commercial Code Signing 1.3.6.2.1.311.2.1.22	"0"	-	-	OID 1.3.6.1.4.1.311.2.1. 22
5.1.11.9 Microsoft Encrypting File System 1.3.6.2.1.31136.10.3.4	"1"	-	-	OID 1.3.6.1.4.1.311.10.3 .4
5.1.12 CRL Distribution Points		√	-	OID 2.5.29.31
5.1.12.1 CRL Distribution Point 1	URL=http://crl.gse.co/sub/crl_gse_sub001_sha2.crl	√	-	
5.1.12.2 CRL Distribution Point 2	URL=http://crl1.gse.co/sub/crl_gse_sub001_sha2.crl	√	-	
5.1.13 qcStatements	No está presente	-	-	OID 1.3.6.1.5.5.7.1.3
5.1.13.1 id-etsi-qcs-QcCompliance	No está presente	-	-	
5.1.13.2 id-etsi-qcs-QcLimitValue	No está presente	-	-	
5.1.13.3 id-etsi-qcs-QcSSCD	No está presente	-	-	
5.1.14 Netscape Cert Type	No está presente	√	-	
5.1.15 Netscape Revocation URL	No está presente	-	-	
5.1.16 Netscape CA Policy URL	No está presente	-	-	
5.1.17 Netscape Comment	No está presente	-	-	
5.1.18 biometricInfo	No está presente	-	-	

5.1.19 Inhibit Any-Policy	No está presente	-	-	
5.1.20 Freshest CRL	No está presente	-	-	
5.2 Internet Certificate Extensions				
5.2.1 Authority Information Access 1		√	-	OID 1.3.6.1.5.5.7.1.1
5.2.1.1 accessMethod	Certification Authority Issuer (1.3.6.1.5.5.7.48.2)	√	-	
5.2.1.2 accessLocation	URI:http://certs.gse.co/sub/crt_gse_sub001_sha2.crt	√	-	
5.2.2 Authority Information Access 2		-	-	
5.2.2.1 accessMethod	On-line Certificate Status Protocol (1.3.6.1.5.5.7.48.1)	-	-	
5.2.2.2 accessLocation	URI:http://ocsp.gse.co	-	-	
5.2.3 Subject Information Access	No está presente	-	-	
6 PKCS#12				
6.1. Friendly Name		-	-	Asignado por la plataforma al momento de generar el certificado. SERIAL NUMBER GIVEN NAME SURNAME
7 Huella Digital				
7.1 Thumbprint algorithm	SHA1	√	X	
7.2 Thumbprint		√	X	Asignado por la plataforma al momento de generar el certificado

8. CERTIFICADO DE PERSONA JURIDICA

CERTIFICADO DE PERSONA JURIDICA HARDWARE / FIRMA CENTRALIZADA				
Campo	**Contenido**	**Obligatorio**	**Crítico**	**Observaciones**
1 TBSCertificate				
1.1 Versión	V3	√	X	[RFC5280]
1.2 Serial number		√	X	Asignado por la plataforma al momento de generar el certificado
1.3 Signature algorithm	Sha256RSA	√	X	OID 1.2.840.113549.1.1.11
1.4 Signature hash algorithm	SHA256	√	X	
2 Issuer				
2.1 Email (E)	ca@gse.co	√	-	
2.2 Common Name (CN)	GSE SUB001_CO	√	X	OID 2.5.4.3
2.3 Organization	GESTION DE SEGURIDAD ELECTRONICA S.A. - GSE	√	-	OID 2.5.4.10
2.4 Serial Number	9002042728	√	-	OID 2.5.4.5
2.5 Organizational Unit	Internet Certification Authority http://www.gse.co	√	-	OID 2.5.4.11
2.6 Title	Subordinate Certificate			OID 2.5.4.12
2.7 StreetAddress	http://www.gse.co/address	√	-	OID 2.5.4.9
2.8 Locality	BOGOTÁ, D.C.	√	-	OID 2.5.4.7
2.9 Country	CO	√	X	OID 2.5.4.6
2.10 Description	GSE Subordinate Certificate 001 Colombia HW-KUSU	√	-	OID 2.5.4.13
3 Validity				

3.1 notBefore		√	X	Asignado por la plataforma al momento de generar el certificado - UTC Time - 5
3.2 notAfter		√	X	Asignado por la plataforma al momento de generar el certificado - UTC Time - 5
4 Subject				
4.1 Description	Certificado de Persona Jurídica - Emitido por GSE SUB001_CO	√	-	OID 2.5.4.13
4.2 Common Name (CN)	Razón Social de la organización	√	-	OID 2.5.4.3 Razón Social de la organización
4.3 1.3.6.1.4.1.31136.2.2.1.2.2	Tipo de Identificación de la Empresa	√	-	Tipo de Identificación de la Empresa
4.4 Serial Number	Número de Identificación de la Empresa	√	-	OID 2.5.4.5 Número de Identificación de la Empresa
4.5 1.3.6.1.4.1.31136.2.2.1.2.4	Entidad donde se registra la empresa	√	-	(Opcional) Entidad encargada de registrar la empresa ejemplo Cámara de comercio, superintendencia, etc.
4.6 Email Address	Email empresa	√	-	Email empresa
4.7 Locality	Municipio / Ciudad de la organización Suscriptor	√	-	OID 2.5.4.7 Municipio / ciudad de la empresa
4.8 StreetAddress	Dirección de la Organización	√	-	OID 2.5.4.9 Dirección de la empresa
4.9 Country	Nacionalidad del Suscriptor	√	-	OID 2.5.4.6 Nacionalidad de la empresa; Código de país de dos dígitos según ISO 3166-1.
4.10 StateOrProvinceName	Estado / Departamento de la organización del suscriptor	√	-	OID 2.5.4.8 Departamento / Estado de la empresa
4.11 Organization	Operado por Razón Social de la empresa	√	-	OID 2.5.4.10 Nombre o Razón social de la empresa
4.12 Given Name	Nombre del responsable **(Si aplica)**	√	-	OID 2.5.4.42 NOMBRE1 NOMBRE2 (en mayúsculas sin separadores entre los nombres) del responsable **(Si aplica)**

4.13 Surname	Apellidos del responsable **(Si aplica)**	√	-	OID 2.5.4.4 APELLIDO1 APELLIDO2 (en mayúsculas sin separadores entre los apellidos) del responsable **(Si aplica)**
4.14 Title	Uso del certificado	√	-	OID 2.5.4.12 uso del certificado
4.15 Organizational Unit (OU)	Cargo del Responsable **(Si aplica)**	√	-	OID 2.5.4.12 Cargo del responsable en la organización **(Si aplica)**
4.16 Subject Publica Key Info	RSAEncryption Clave Pública de 2048 bits (RF3279) Clave Pública de 2048 bits (RF3279)	√	X	OID 1.2.840.113549.1.1.1 Clave pública de 2048 bits [RFC3279]
4.17 Public key parameters	"0500"	√	X	
5 Extensions				
5.1 Standard Extensions				
5.1.1 Authority Key Identifier	KeyID=8e 4a 03 5e a3 fd 09 a7 63 b5 64 ee 75 46 7a 6c dd be 45 49	√	X	OID 2.5.29.35
5.1.1.1 keyIdentifier		√	-	
5.1.1.2 authorityCertIssuer		√	-	
5.1.1.3 authorityCertSerialNumber		√	-	
5.1.2 Subject Key Identifier		√	-	OID 2.5.29.14
5.1.3 Key Usage		√	-	OID 2.5.29.15
5.1.3.1 digitalSignature	"1"	X	-	
5.1.3.2 nonRepudiation-ContentCommitment	"1"	X	-	

5.1.3.3 keyEncipherment	"1"	X	-	
5.1.3.4 dataEncipherment	"1"	X	-	
5.1.3.5 keyAgreement	"1"	X	-	
5.1.3.6 keyCertSign	"0"	√	-	
5.1.3.7 cRLSign	"0"	√	-	
5.1.3.8 encipherOnly	"0"	X	-	
5.1.3.9 decipherOnly	"0"	X	-	
5.1.4 Certificate Policies		√	X	OID 2.5.29.32
5.1.4.1 Policy Identifier	1.3.6.1.4.1.31136.2.2.3.10.2 - En token 1.3.6.1.4.1.31136.2.2.3.10.3 - En HSM	√	-	OID Definido por ECD GSE
5.1.4.2 Policy Qualifier ID		√	-	
5.1.4.2.1 CPS Pointer	http://cps.gse.co/sub/cps_sub001_ca_gse.pdf	√	-	OID 1.3.6.1.5.5.7.2.1
5.1.4.2.2 User Notice	Terms of use at CPS CA GSE http://cps.gse.co/sub/cps_sub001_ca_gse.pdf	√	-	
5.1.5 Subject Alternative Name				
5.1.6 Issuer Alternative Name	URI:http://www.gse.co	√	X	OID 2.5.29.18
5.1.7 Subject Directory Attributes	No está presente	X	X	OID 2.5.29.9

5.1.8 Basic Constraints		√	√	
5.1.8.1 cA	End Entity	√	-	
5.1.8.2 pathLenConstraint	No está presente	√	-	
5.1.9 Name Constraints	No está presente	X	X	
5.1.10 Policy Constraints	No está presente	X	X	
5.1.11 Extended Key Usage	No está presente	X	X	OID 2.5.29.37
5.1.11.1 serverAuth	"0"	-	-	OID 1.3.6.1.5.5.7.3.1
5.1.11.2 clientAuth	"1"	-	-	OID 1.3.6.1.5.5.7.3.2
5.1.11.3 codeSigning	"0"	-	-	OID 1.3.6.1.5.5.7.3.3
5.1.11.4 emailProtection	"1"	-	-	OID 1.3.6.1.5.5.7.3.4
5.1.11.5 timeStamping	"0"	-	-	OID 1.3.6.1.5.5.7.3.8
5.1.11.6 OCSPSigning	"0"	-	-	OID 1.3.6.1.5.5.7.3.9
5.1.11.7 Microsoft Smart Card Logon for Windows 1.3.6.2.1.311.20.2.2	"1"	-	-	OID 1.3.6.1.4.1.311.20.2 .2
5.1.11.8 Microsoft Commercial Code Signing 1.3.6.2.1.311.2.1.22	"0"	-	-	OID 1.3.6.1.4.1.311.2.1. 22

5.1.11.9 Microsoft Encrypting File System 1.3.6.2.1.31136.10.3.4	"1"	-	-	OID 1.3.6.1.4.1.311.10.3 .4
5.1.12 CRL Distribution Points		√	-	OID 2.5.29.31
5.1.12.1 CRL Distribution Point 1	URL=http://crl.gse.co/sub/crl_gse_sub001_sha2.crl	√	-	
5.1.12.2 CRL Distribution Point 2	URL=http://crl1.gse.co/sub/crl_gse_sub001_sha2.crl	√	-	
5.1.13 qcStatements	No está presente	-	-	OID 1.3.6.1.5.5.7.1.3
5.1.13.1 id-etsi-qcs-QcCompliance	No está presente	-	-	
5.1.13.2 id-etsi-qcs-QcLimitValue	No está presente	-	-	
5.1.13.3 id-etsi-qcs-QcSSCD	No está presente	-	-	
5.1.14 Netscape Cert Type	No está presente	√	-	
5.1.15 Netscape Revocation URL	No está presente	-	-	
5.1.16 Netscape CA Policy URL	No está presente	-	-	
5.1.17 Netscape Comment	No está presente	-	-	
5.1.18 biometricInfo	No está presente	-	-	
5.1.19 Inhibit Any-Policy	No está presente	-	-	
5.1.20 Freshest CRL	No está presente	-	-	
5.2 Internet Certificate Extensions				

5.2.1 Authority Information Access 1		√	-	OID 1.3.6.1.5.5.7.1.1
5.2.1.1 accessMethod	Certification Authority Issuer (1.3.6.1.5.5.7.48.2)	√	-	
5.2.1.2 accessLocation	URI:http://certs.gse.co/sub/crt_gse_sub001_sha2.crt	√	-	
5.2.2 Authority Information Access 2		-	-	
5.2.2.1 accessMethod	On-line Certificate Status Protocol (1.3.6.1.5.5.7.48.1)	-	-	
5.2.2.2 accessLocation	URI:http://ocsp.gse.co	-	-	
5.2.3 Subject Information Access	No está presente	-	-	
6 PKCS#12				
6.1. Friendly Name		-	-	Asignado por la plataforma al momento de generar el certificado. SERIAL NUMBER GIVEN NAME SURNAME
7 Huella Digital				
7.1 Thumbprint algorithm	SHA1	√	X	
7.2 Thumbprint		√	X	Asignado por la plataforma al momento de generar el certificado

9. CERTIFICADO DE SECTOR EDUCATIVO HARDWARE / FIRMA CENTRALIZADA

CERTIFICADO DE SECTOR EDUCATIVO HARDWARE

GESTIÓN DE SEGURIDAD ELECTRÓNICA	**Anexo 1** **Perfil técnico certificados digitales GSE SUB001_CO**	Fecha de vigencia	27/11/2018
		Versión	3

Campo	Contenido	Obligatorio	Crítico	Observaciones
1 TBSCertificate				
1.1 Versión	V3	√	X	[RFC5280]
1.2 Serial number		√	X	Asignado por la plataforma al momento de generar el certificado
1.3 Signature algorithm	Sha256RSA	√	X	OID 1.2.840.113549.1.1.11
1.4 Signature hash algorithm	SHA256	√	X	
2 Issuer				
2.1 Email (E)	ca@gse.co	√	-	
2.2 Common Name (CN)	GSE SUB001_CO	√	X	OID 2.5.4.3
2.3 Organization	GESTION DE SEGURIDAD ELECTRONICA S.A. - GSE	√	-	OID 2.5.4.10
2.4 Serial Number	9002042728	√	-	OID 2.5.4.5
2.5 Organizational Unit	Internet Certification Authority http://www.gse.co	√	-	OID 2.5.4.11
2.6 Title	Subordinate Certificate			OID 2.5.4.12
2.7 StreetAddress	http://www.gse.co/address	√	-	OID 2.5.4.9
2.8 Locality	BOGOTÁ, D.C.	√	-	OID 2.5.4.7
2.9 Country	CO	√	X	OID 2.5.4.6
2.10 Description	GSE Subordinate Certificate 001 Colombia HW-KUSU	√	-	OID 2.5.4.13
3 Validity				
3.1 notBefore		√	X	Asignado por la plataforma al momento de generar el certificado - UTC Time - 5
3.2 notAfter		√	X	Asignado por la plataforma al momento de generar el certificado - UTC Time - 5

4 Subject				
4.1 Description	Certificado de Sector Educativo - Emitido por GSE SUB001_CO	√	-	OID 2.5.4.13
4.2 Common Name (CN)	Nombre y apellidos del suscriptor	√	-	OID 2.5.4.3 APELLIDO1 APELLIDO2 NOMBRE1 NOMBRE2 (en mayúsculas sin separadores entre los apellidos y los nombres)
4.3 1.3.6.1.4.1.31136.2.2.1.2.1	Tipo de Identificación Personal	√	-	Tipo de Identificación Personal
4.4 Serial Number	Número de documento del suscriptor	√	-	OID 2.5.4.5 Numero de documento
4.5 Email Address	Email del suscriptor	√	-	Email del suscriptor
4.6 1.3.6.1.4.1.31136.2.2.1.2.12	Código identificador	√	-	Código interno del cliente
4.7 Title	Area del Sector Educativo	√	-	OID 2.5.4.12 "Estudiantes, Profesor, Rector, Coordinador, Docente, Pasante, Administración"
4.8 Organization	Nombre o Razón Social de la Institución	√	-	OID 2.5.4.10 Nombre o Razón social de la empresa
4.9 StreetAddress	Dirección de la institución	√	-	OID 2.5.4.9 Dirección de la empresa
4.10 StateOrProvinceName	Estado / Departamento del suscriptor	√	-	OID 2.5.4.8 Departamento / Estado de la empresa
4.11 Locality	Municipio / Ciudad del Suscriptor	√	-	OID 2.5.4.7 Municipio / ciudad de la empresa
4.12 Surname	Apellidos del suscriptor	√	-	OID 2.5.4.4 APELLIDO1 APELLIDO2 (en mayúsculas sin separadores entre los apellidos)
4.13 Given Name	Nombre de suscriptor	√	-	OID 2.5.4.42 NOMBRE1 NOMBRE2 (en mayúsculas sin separadores entre los nombres)
4.14 Country	Nacionalidad del Suscriptor	√	-	OID 2.5.4.6 Nacionalidad del Suscriptor; Código de país de dos dígitos según ISO 3166-1.
4.15 Subject Publica Key Info	RSAEncryption Clave Pública de 2048 bits (RF3279) Clave Pública de 2048 bits (RF3279)	√	X	OID 1.2.840.113549.1.1.1 Clave pública de 2048 bits [RFC3279]

4.16 Public key parameters	"0500"	√	X	
5 Extensions				
5.1 Standard Extensions				
5.1.1 Authority Key Identifier	KeyID=8e 4a 03 5e a3 fd 09 a7 63 b5 64 ee 75 46 7a 6c dd be 45 49	√	X	OID 2.5.29.35
5.1.1.1 keyIdentifier		√	-	
5.1.1.2 authorityCertIssuer		√	-	
5.1.1.3 authorityCertSerialNumber		√	-	
5.1.2 Subject Key Identifier		√	-	OID 2.5.29.14
5.1.3 Key Usage		√	-	OID 2.5.29.15
5.1.3.1 digitalSignature	"1"	X	-	
5.1.3.2 nonRepudiation-ContentCommitment	"1"	X	-	
5.1.3.3 keyEncipherment	"1"	X	-	
5.1.3.4 dataEncipherment	"1"	X	-	
5.1.3.5 keyAgreement	"1"	X	-	
5.1.3.6 keyCertSign	"0"	√	-	
5.1.3.7 cRLSign	"0"	√	-	

5.1.3.8 encipherOnly	"0"	X	-	
5.1.3.9 decipherOnly	"0"	X	-	
5.1.4 Certificate Policies		√	X	OID 2.5.29.32
5.1.4.1 Policy Identifier	1.3.6.1.4.1.31136.2.2.3.8.2 -En token	√	-	OID Definido por ECD GSE
5.1.4.2 Policy Qualifier ID		√	-	
5.1.4.2.1 CPS Pointer	http://cps.gse.co/sub/cps_sub001_ca_gse.pdf	√	-	OID 1.3.6.1.5.5.7.2.1
5.1.4.2.2 User Notice	Terms of use at CPS CA GSE http://cps.gse.co/sub/cps_sub001_ca_gse.pdf	√	-	
5.1.5 Subject Alternative Name				
5.1.6 Issuer Alternative Name	URI:http://www.gse.co	√	X	OID 2.5.29.18
5.1.7 Subject Directory Attributes	No está presente	X	X	OID 2.5.29.9
5.1.8 Basic Constraints		√	√	
5.1.8.1 cA	End Entity	√	-	
5.1.8.2 pathLenConstraint	No está presente	√	-	
5.1.9 Name Constraints	No está presente	X	X	
5.1.10 Policy Constraints	No está presente	X	X	

5.1.11 Extended Key Usage	No está presente	X	X	OID 2.5.29.37
5.1.11.1 serverAuth	"0"	-	-	OID 1.3.6.1.5.5.7.3.1
5.1.11.2 clientAuth	"1"	-	-	OID 1.3.6.1.5.5.7.3.2
5.1.11.3 codeSigning	"0"	-	-	OID 1.3.6.1.5.5.7.3.3
5.1.11.4 emailProtection	"1"	-	-	OID 1.3.6.1.5.5.7.3.4
5.1.11.5 timeStamping	"0"	-	-	OID 1.3.6.1.5.5.7.3.8
5.1.11.6 OCSPSigning	"0"	-	-	OID 1.3.6.1.5.5.7.3.9
5.1.11.7 Microsoft Smart Card Logon for Windows 1.3.6.2.1.311.20.2.2	"1"	-	-	OID 1.3.6.1.4.1.311.20.2 .2
5.1.11.8 Microsoft Commercial Code Signing 1.3.6.2.1.311.2.1.22	"0"	-	-	OID 1.3.6.1.4.1.311.2.1. 22
5.1.11.9 Microsoft Encrypting File System 1.3.6.2.1.31136.10.3.4	"1"	-	-	OID 1.3.6.1.4.1.311.10.3 .4
5.1.12 CRL Distribution Points		√	-	OID 2.5.29.31
5.1.12.1 CRL Distribution Point 1	URL=http://crl.gse.co/sub/crl_gse_sub001_sha2.crl	√	-	
5.1.12.2 CRL Distribution Point 2	URL=http://crl1.gse.co/sub/crl_gse_sub001_sha2.crl	√	-	
5.1.13 qcStatements	No está presente	-	-	OID 1.3.6.1.5.5.7.1.3

5.1.13.1 id-etsi-qcs-QcCompliance	No está presente	-	-	
5.1.13.2 id-etsi-qcs-QcLimitValue	No está presente	-	-	
5.1.13.3 id-etsi-qcs-QcSSCD	No está presente	-	-	
5.1.14 Netscape Cert Type	No está presente	√	-	
5.1.15 Netscape Revocation URL	No está presente	-	-	
5.1.16 Netscape CA Policy URL	No está presente	-	-	
5.1.17 Netscape Comment	No está presente	-	-	
5.1.18 biometricInfo	No está presente	-	-	
5.1.19 Inhibit Any-Policy	No está presente	-	-	
5.1.20 Freshest CRL	No está presente	-	-	
5.2 Internet Certificate Extensions				
5.2.1 Authority Information Access 1		√	-	OID 1.3.6.1.5.5.7.1.1
5.2.1.1 accessMethod	Certification Authority Issuer (1.3.6.1.5.5.7.48.2)	√	-	
5.2.1.2 accessLocation	URI:http://certs.gse.co/sub/crt_gse_sub001_sha2.crt	√	-	
5.2.2 Authority Information Access 2		-	-	
5.2.2.1 accessMethod	On-line Certificate Status Protocol (1.3.6.1.5.5.7.48.1)	-	-	

5.2.2.2 accessLocation	URI:http://ocsp.gse.co	-	-	
5.2.3 Subject Information Access	No está presente	-	-	
6 PKCS#12				
6.1. Friendly Name		-	-	Asignado por la plataforma al momento de generar el certificado. SERIAL NUMBER GIVEN NAME SURNAME
7 Huella Digital				
7.1 Thumbprint algorithm	SHA1	√	X	
7.2 Thumbprint		√	X	Asignado por la plataforma al momento de generar el certificado

10. CERTIFICADO DE CORREO ELECTRONICO HARDWARE

CERTIFICADO DE CORREO ELECTRONICO				
Campo	**Contenido**	**Obligatorio**	**Crítico**	**Observaciones**
1 TBSCertificate				
1.1 Versión	V3	√	X	[RFC5280]
1.2 Serial number		√	X	Asignado por la plataforma al momento de generar el certificado
1.3 Signature algorithm	Sha256RSA	√	X	OID 1.2.840.113549.1.1.11
1.4 Signature hash algorithm	SHA256	√	X	
2 Issuer				
2.1 Email (E)	ca@gse.co	√	-	

2.2 Common Name (CN)	GSE SUB001_CO	√	X	OID 2.5.4.3
2.3 Organization	GESTION DE SEGURIDAD ELECTRONICA S.A. - GSE	√	-	OID 2.5.4.10
2.4 Serial Number	9002042728	√	-	OID 2.5.4.5
2.5 Organizational Unit	Internet Certification Authority http://www.gse.co	√	-	OID 2.5.4.11
2.6 Title	Subordinate Certificate			OID 2.5.4.12
2.7 StreetAddress	http://www.gse.co/address	√	-	OID 2.5.4.9
2.8 Locality	BOGOTÁ, D.C.	√	-	OID 2.5.4.7
2.9 Country	CO	√	X	OID 2.5.4.6
2.10 Description	GSE Subordinate Certificate 001 Colombia HW-KUSU	√	-	OID 2.5.4.13
3 Validity				
3.1 notBefore		√	X	Asignado por la plataforma al momento de generar el certificado - UTC Time - 5
3.2 notAfter		√	X	Asignado por la plataforma al momento de generar el certificado - UTC Time - 5
4 Subject				
4.1 Description	Certificado de Correo Electrónico - Emitido por GSE SUB001_CO	√	-	OID 2.5.4.13
4.2 Common Name (CN)	Nombre y apellidos del suscriptor	√	-	OID 2.5.4.3 APELLIDO1 APELLIDO2 NOMBRE1 NOMBRE2 (en mayúsculas sin separadores entre los apellidos y los nombres)
4.3 1.3.6.1.4.1.31136.2.2.1.2.1	Tipo de Identificación Personal	√	-	Tipo de Identificación Personal
4.4 Serial Number	Número de documento del suscriptor	√	-	OID 2.5.4.5 Numero de documento
4.5 Email Address	Email del suscriptor	√	-	Email del suscriptor
4.12 StreetAddress	Dirección del Suscriptor	√	-	OID 2.5.4.9 Dirección de la empresa

4.13 StateOrProvinceName	Estado / Departamento del Suscriptor	√	-	OID 2.5.4.8 Departamento / Estado de la empresa
4.14 Locality	Municipio / Ciudad del Suscriptor	√	-	OID 2.5.4.7 Municipio / ciudad de la empresa
4.15 Surname	Apellidos del suscriptor	√	-	OID 2.5.4.4 APELLIDO1 APELLIDO2 (en mayúsculas sin separadores entre los apellidos)
4.16 Given Name	Nombre de suscriptor	√	-	OID 2.5.4.42 NOMBRE1 NOMBRE2 (en mayúsculas sin separadores entre los nombres)
4.17 Country	Nacionalidad del Suscriptor	√	-	OID 2.5.4.6 Nacionalidad del Suscriptor; Código de país de dos dígitos según ISO 3166-1.
4.18 Subject Publica Key Info	RSAEncryption Clave Pública de 2048 bits (RF3279) Clave Pública de 2048 bits (RF3279)	√	X	OID 1.2.840.113549.1.1.1 Clave pública de 2048 bits [RFC3279]
4.19 Public key parameters	"0500"	√	X	
5 Extensions				
5.1 Standard Extensions				
5.1.1 Authority Key Identifier	KeyID=8e 4a 03 5e a3 fd 09 a7 63 b5 64 ee 75 46 7a 6c dd be 45 49	√	X	OID 2.5.29.35
5.1.1.1 keyIdentifier		√	-	
5.1.1.2 authorityCertIssuer		√	-	
5.1.1.3 authorityCertSerialNumber		√	-	
5.1.2 Subject Key Identifier		√	-	OID 2.5.29.14
5.1.3 Key Usage		√	-	OID 2.5.29.15
5.1.3.1 digitalSignature	"1"	X	-	

5.1.3.2 nonRepudiation-ContentCommitment	"1"	X	-	
5.1.3.3 keyEncipherment	"1"	X	-	
5.1.3.4 dataEncipherment	"1"	X	-	
5.1.3.5 keyAgreement	"1"	X	-	
5.1.3.6 keyCertSign	"0"	√	-	
5.1.3.7 cRLSign	"0"	√	-	
5.1.3.8 encipherOnly	"0"	X	-	
5.1.3.9 decipherOnly	"0"	X	-	
5.1.4 Certificate Policies		√	X	OID 2.5.29.32
5.1.4.1 Policy Identifier	1.3.6.1.4.1.31136.2.2.3.13.2 - En token	√	-	OID Definido por ECD GSE
5.1.4.2 Policy Qualifier ID		√	-	
5.1.4.2.1 CPS Pointer	http://cps.gse.co/sub/cps_sub001_ca_gse.pdf	√	-	OID 1.3.6.1.5.5.7.2.1
5.1.4.2.2 User Notice	Terms of use at CPS CA GSE http://cps.gse.co/sub/cps_sub001_ca_gse.pdf	√	-	
5.1.5 Subject Alternative Name				
5.1.6 Issuer Alternative Name	URI:http://www.gse.co	√	X	OID 2.5.29.18

5.1.7 Subject Directory Attributes	No está presente	X	X	OID 2.5.29.9
5.1.8 Basic Constraints		√	√	
5.1.8.1 cA	End Entity	√	-	
5.1.8.2 pathLenConstraint	No está presente	√	-	
5.1.9 Name Constraints	No está presente	X	X	
5.1.10 Policy Constraints	No está presente	X	X	
5.1.11 Extended Key Usage	No está presente	X	X	OID 2.5.29.37
5.1.11.1 serverAuth	"0"	-	-	OID 1.3.6.1.5.5.7.3.1
5.1.11.2 clientAuth	"0"	-	-	OID 1.3.6.1.5.5.7.3.2
5.1.11.3 codeSigning	"0"	-	-	OID 1.3.6.1.5.5.7.3.3
5.1.11.4 emailProtection	"1"	-	-	OID 1.3.6.1.5.5.7.3.4
5.1.11.5 timeStamping	"0"	-	-	OID 1.3.6.1.5.5.7.3.8
5.1.11.6 OCSPSigning	"0"	-	-	OID 1.3.6.1.5.5.7.3.9
5.1.11.7 Microsoft Smart Card Logon for Windows 1.3.6.2.1.311.20.2.2	"1"	-	-	OID 1.3.6.1.4.1.311.20.2 .2

5.1.11.8 Microsoft Commercial Code Signing 1.3.6.2.1.311.2.1.22	"0"	-	-	OID 1.3.6.1.4.1.311.2.1. 22
5.1.11.9 Microsoft Encrypting File System 1.3.6.2.1.31136.10.3.4	"1"	-	-	OID 1.3.6.1.4.1.311.10.3 .4
5.1.12 CRL Distribution Points		√	-	OID 2.5.29.31
5.1.12.1 CRL Distribution Point 1	URL=http://crl.gse.co/sub/crl_gse_sub001_sha2.crl	√	-	
5.1.12.2 CRL Distribution Point 2	URL=http://crl1.gse.co/sub/crl_gse_sub001_sha2.crl	√	-	
5.1.13 qcStatements	No está presente	-	-	OID 1.3.6.1.5.5.7.1.3
5.1.13.1 id-etsi-qcs-QcCompliance	No está presente	-	-	
5.1.13.2 id-etsi-qcs-QcLimitValue	No está presente	-	-	
5.1.13.3 id-etsi-qcs-QcSSCD	No está presente	-	-	
5.1.14 Netscape Cert Type	No está presente	√	-	
5.1.15 Netscape Revocation URL	No está presente	-	-	
5.1.16 Netscape CA Policy URL	No está presente	-	-	
5.1.17 Netscape Comment	No está presente	-	-	
5.1.18 biometricInfo	No está presente	-	-	

5.1.19 Inhibit Any-Policy	No está presente	-	-	
5.1.20 Freshest CRL	No está presente	-	-	
5.2 Internet Certificate Extensions				
5.2.1 Authority Information Access 1		√	-	OID 1.3.6.1.5.5.7.1.1
5.2.1.1 accessMethod	Certification Authority Issuer (1.3.6.1.5.5.7.48.2)	√	-	
5.2.1.2 accessLocation	URI:http://certs.gse.co/sub/crt_gse_sub001_sha2.crt	√	-	
5.2.2 Authority Information Access 2		-	-	
5.2.2.1 accessMethod	On-line Certificate Status Protocol (1.3.6.1.5.5.7.48.1)	-	-	
5.2.2.2 accessLocation	URI:http://ocsp.gse.co	-	-	
5.2.3 Subject Information Access	No está presente	-	-	
6 PKCS#12				
6.1. Friendly Name		-	-	Asignado por la plataforma al momento de generar el certificado. SERIAL NUMBER GIVEN NAME SURNAME
7 Huella Digital				
7.1 Thumbprint algorithm	SHA1	√	X	
7.2 Thumbprint		√	X	Asignado por la plataforma al momento de generar el certificado