



PERFILES DE CERTIFICADOS DICERT	
TI	Código: PCD-DC-GG-014
	Versión: 1.0
	Clasificación de Información: Documento INTERNO

PERFILES DE CERTIFICADOS DICERT

Aprobado por:	Firma de Aprobación:
Galo Becerra	
	Fecha de Aprobación: 6 de febrero de 2026

	PERFILES DE CERTIFICADOS DICERT	
	Revisado: Galo Becerra - GG	Código: PCD-DC-GG-014
		Versión: 2.0
		Clasificación de Información: DOCUMENTO CONFIDENCIAL

Contenido/ Índice

Control de Cambios.....	2
1. Perfil Certificado de Persona Natural en Archivo.....	2
2. Perfil Certificado de Miembro de Empresa o Empleado con Relación de Dependencia en Archivo.....	6
3. Perfil Certificado de Representante Legal en Archivo.....	10
4. Perfil Certificado de Sello Electrónico en Archivo.....	13
5. Perfil Certificado de Sellado de Tiempo.....	17
6. Perfil Certificado de Certificado Raíz AC Root.....	21
7. Perfil Certificado de Certificado Subordinado AC Sub.....	23
8. Perfil Certificado de Certificado de Validación OCSP.....	26

 Certificamos Información Digital	PERFILES DE CERTIFICADOS DICERT		
	Revisado: Galo Becerra - GG	Código: PCD-DC-GG-014	
		Versión: 2.0	
		Clasificación de Información: DOCUMENTO CONFIDENCIAL	

Control de Cambios

VERSIÓN	DETALLE	ELABORADO POR:	FECHA APROBACIÓN	REVISADO POR:
1.0	Versión Inicial	Tamara Isch	08-04-2024	Galo Becerra
2.0	Actualización Reforma Legal	Tamara Isch	05-02-2026	Galo Becerra

1. Perfil Certificado de Persona Natural en Archivo

PERSONA NATURAL EN ARCHIVO - ANEXO 1A				
Campo	En Archivo	Obligatorio	Crítico	Observaciones 1.3.6.1.4.1.62486.2.1.1
De persona Natural	Autenticación y Firma			
1. Basic structure				
1.1. Version	"2"	SI		El literal “2” corresponde a la versión 3. X.509
1.2. Serial Number	Establecido automáticamente por la AC Número identificativo único del certificado.	SI		No puede ser un número negativo ni 0.
1.3. Signature Algorithm		SI		
1.3.1. Algorithm	SHA-256 with RSA Signature	SI		1.2.840.113549.1.1.11
1.3.2. Parameters	No aplicable	NO		
1.4. Issuer		SI		
1.4.1. Country Name (C)	Código del País "EC" (ISO 3166)	SI		OID 2.5.4.6
1.4.2. Organization Name (O)	DICERT S.A.	SI		OID 2.5.4.10
1.4.3. Locality Name (L)	QUITO	SI		OID 2.5.4.7
1.4.4. Organization Identifier	VATEC-1793151884001	NO		OID 2.5.4.97 codificación acorde la ETSI EN 319 412-1 RFC 5280 establece como no obligatorio
1.4.5. Common Name (CN)	Nombre de la AC Subordinada "DICERT AC SUBORDINADA"	SI		OID 2.5.4.3
1.4.6. Organizational Unit Name (OU)	UNIDAD DE CERTIFICACION ELECTRONICA	NO		OID 2.5.4.11

 Certificamos Información Digital	PERFILES DE CERTIFICADOS DICERT		
	Revisado: Galo Becerra - GG	Código: PCD-DC-GG-014	
		Versión: 2.0	
		Clasificación de Información: DOCUMENTO CONFIDENCIAL	

1.5. Validity		SI		
1.5.1. Not Before	Fecha de inicio de validez	SI		YYMMDDHHMMSSZ
1.5.2. Not After	Fecha de expiración	SI		YYMMDDHHMMSSZ
1.6. Subject		SI		
1.6.1. Country Name (C)	EC	SI		OID 2.5.4.6
1.6.2. Locality Name (L)	Localidad del Titular de la Firma (Ciudad) ej. QUITO	SI		OID 2.5.4.7
1.6.3. Title	Título o especialidad del Titular de la Firma	NO		OID 2.5.4.12
1.6.4. Surname	Apellidos del Titular de la Firma (como consta en el documento oficial)	SI		OID 2.5.4.4
1.6.5. Given Name	Nombres del Titular de la firma (como consta en el documento oficial)	SI		OID 2.5.4.42
1.6.6. Serial Number	Número de cédula (IDC"País"-1716151413) o pasaporte (PAS"País"-A6362611) Ej. IDCEC-1716151413 o PASEC-A6362611	SI		OID 2.5.4.5 Número de documento oficial codificado acorde a ETSI EN 319 412-1
1.6.7. Organization Identifier	Número de Registro Unico de Contribuyente TIN(CÓDIGO_PAÍS)-RUC Ej. ("TINEC-1716151413001")	NO		OID 2.5.4.97 codificación acorde la ETSI EN 319 412-1 RFC 5280 establece como no obligatorio
1.6.8. Common Name (CN)	Nombres y Apellidos del Titular de la Firma	SI		OID 2.5.4.3
1.7. Subject Public Key Info		SI		
1.7.1. AlgorithmIdentifier				
1.7.1.1. Algorithm	RSA encryption	SI		OID 1.2.840.113549.1.1.1
1.7.1.2. Parameters	No aplicable	NO		
1.7.2. SubjectPublicKey	Clave pública del Titular de la Firma	SI		Acorde ETSI TS 119 312
2. Extensions				
2.1. Authority Key Identifier	Identificador de la clave del Issuer	NO	NO	OID 2.5.29.35 (Marcado como NO crítico según EN 319412-2) No es obligatorio siempre y cuando la clave pública de la AC se distribuya en forma de certificado "AUTOFIRMADO"

 Certificamos Información Digital	PERFILES DE CERTIFICADOS DICERT		
	Revisado: Galo Becerra - GG	Código: PCD-DC-GG-014	
		Versión: 2.0	
		Clasificación de Información: DOCUMENTO CONFIDENCIAL	

2.1.1. KeyIdentifier		NO		Derivado de la clave pública
2.2. Subject Key Identifier	Identificador de la clave del Subject	SI	NO	OID 2.5.29.14 (Marcado como NO crítico según EN 319412-2)
2.2.1. KeyIdentifier		SI		Derivado de la clave pública
2.3. Key Usage		SI	SI	OID 2.5.29.15
2.3.1. Digital Signature	Seleccionado "1"	SI		
2.3.2. Content commitment	Seleccionado "1"	SI		
2.3.3. Key Encipherment	Seleccionado "1"	SI		
2.3.4. Data Encipherment	No seleccionado. "0"			
2.3.5. Key Agreement	No seleccionado. "0"			
2.3.6. Key Certificate Signature	No seleccionado. "0"			
2.3.7. CRL Signature	No seleccionado. "0"			
2.3.8. Encipher Only	No seleccionado. "0"			
2.3.9. Decipher Only	No seleccionado. "0"			
2.4. Certificate Policies		SI	NO	OID 2.5.29.32 (Marcado como NO crítico según EN 319412-2)
2.4.1. Policy Information		SI		
2.4.1.1. Policy Identifier	1.3.6.1.4.1.oid_AC.2.6.1	SI		Identificador de la política de la AC
2.4.1.2. Policy Qualifiers		SI		
2.4.1.1.1 CPS URI	https://dicert.com.ec/links/dpc	SI		OID 1.3.6.1.5.5.7.2.1 URL de la Política de Certificados de la Entidad Acreditada
2.4.1.1.2. User Notice/Explicit text	"CERTIFICADO DE PERSONA NATURAL EN ARCHIVO"	SI		OID 1.3.6.1.5.5.7.2.2 Texto indicativo
2.5. Subject Alternative Names		NO	NO	OID 2.5.29.17 (Marcado como NO crítico según EN 319412-2)
2.5.1. rfc822Name	Correo electrónico del Titular de la Firma nombreapellido@example.com.ec	SI		
2.6. Extended Key Usage		SI	NO	OID 2.5.29.37 (Marcado como NO crítico según EN 319412-2)
2.6.1. clientAuth	Presente (1.3.6.1.5.5.7.3.2)	SI		Transport Layer Security (TLS) World Wide Web (WWW)

 Certificamos Información Digital	PERFILES DE CERTIFICADOS DICERT		
	Revisado: Galo Becerra - GG	Código: PCD-DC-GG-014	
		Versión: 2.0	
		Clasificación de Información: DOCUMENTO CONFIDENCIAL	

				client authentication
2.6.2. Email protection	Presente (1.3.6.1.5.5.7.3.4)	SI		Sí se incluye el correo electrónico del Titular de la Firma
2.7. cRLDistributionPoint		NO	NO	OID 2.5.29.31 (Marcado como NO crítico según EN 319412-2)
2.7.1. distributionPoint	https://dicert.com.ec/links/crl1	SI		http (http://) IETF RFC 7230-7235 [3] or ldap (ldap://) IETF RFC 4516 [4] scheme
2.7.2. distributionPoint	https://dicert.com.ec/links/crl2	NO		http (http://) IETF RFC 7230-7235 [3] or ldap (ldap://) IETF RFC 4516 [4] scheme
2.8. Authority Information Access		SI	NO	OID 1.3.6.1.5.5.7.1.1 (Marcado como NO crítico según EN 319412-2)
2.8.1. Access Description		SI		
2.8.1.1. Access Method	id-ad-ocsp	SI		OID 1.3.6.1.5.5.7.48.1
2.8.1.1.1 Access Location	https://dicert.com.ec/links/ocsp	SI		URL de acceso al OCSP (http://) IETF RFC 7230-7235 [3] or https (https://) IETF RFC 2818 [5]
2.8.1.1.2 Access Location		NO		URL de acceso al OCSP (http://) IETF RFC 7230-7235 [3] or https (https://) IETF RFC 2818 [5]
2.8.2. Access Description		NO		No es obligatorio siempre y cuando incluya la ubicación de acceso al OCSP
2.8.2.1. Access Method	id-ad-calssuers	NO		OID 1.3.6.1.5.5.7.48.2
2.8.2.1.1 Access Location	https://dicert.com.ec/links/certac	NO		URL acceso a certificado de la AC (http://) IETF RFC 7230-7235 [3] or https (https://) IETF RFC 2818 [5]
2.9. Basic Constraints		SI	SI	OID 2.5.29.19
2.9.1. cA	FALSE	SI		

	PERFILES DE CERTIFICADOS DICERT		
	Revisado: Galo Becerra - GG	Código: PCD-DC-GG-014	
		Versión: 2.0	
		Clasificación de Información: DOCUMENTO CONFIDENCIAL	

2. Perfil Certificado de Miembro de Empresa o Empleado con Relación de Dependencia en Archivo

MIEMBRO DE EMPRESA O EMPLEADO CON RELACIÓN DE DEPENDENCIA EN ARCHIVO - ANEXO 2A				
Campo	En Archivo	Obligatorio	Crítico	Observaciones 1.3.6.1.4.1.62486.2.2.1
De Miembro de Empresa o de Relación de Dependencia	Autenticación y Firma			
1. Basic structure				
1.1. Version	"2"	SI		El literal “2” corresponde a la versión 3. X.509
1.2. Serial Number	Establecido automáticamente por la AC Número identificativo único del certificado.	SI		No puede ser un número negativo ni 0.
1.3. Signature Algorithm		SI		
1.3.1. Algorithm	SHA-256 with RSA Signature	SI		1.2.840.113549.1.1.11
1.3.2. Parameters	No aplicable	NO		
1.4. Issuer		SI		
1.4.1. Country Name (C)	Código del País "EC" (ISO 3166)	SI		OID 2.5.4.6
1.4.2. Organization Name (O)	DICERT S.A.	SI		OID 2.5.4.10
1.4.3. Locality Name (L)	QUITO	SI		OID 2.5.4.7
1.4.4. Organization Identifier	VATEC-1793151884001	NO		OID 2.5.4.97 codificación acorde la ETSI EN 319 412-1 RFC 5280 establece como no obligatorio
1.4.5. Common Name (CN)	Nombre de la AC Subordinada "DICERT AC SUBORDINADA"	SI		OID 2.5.4.3
1.4.6. Organizational Unit Name (OU)	UNIDAD DE CERTIFICACION ELECTRONICA	NO		OID 2.5.4.11
1.5. Validity		SI		
1.5.1. Not Before	Fecha de inicio de validez	SI		YYMMDDHHMMSSZ
1.5.2. Not After	Fecha de expiración	SI		YYMMDDHHMMSSZ
1.6. Subject		SI		
1.6.1. Country Name (C)	EC	SI		OID 2.5.4.6

 Certificamos Información Digital	PERFILES DE CERTIFICADOS DICERT		
	Revisado: Galo Becerra - GG		Código: PCD-DC-GG-014
			Versión: 2.0
			Clasificación de Información: DOCUMENTO CONFIDENCIAL

1.6.2. Locality Name (L)	Localidad del Signatario (Ciudad) ej. QUITO	SI		OID 2.5.4.7
1.6.3. Organization Name (O)	Se especificará el nombre de la Persona Natural o Persona Jurídica (Pública o Privada) a la que pertenece el Signatario o con quien tiene relación de dependencia. Ej. CORPORACION FAVORITA	SI		OID 2.5.4.10
1.6.4. Organizational Unit Name (OU)	Se especificará el Departamento o Área al que pertenece el Signatario o el tipo de vinculación con la Persona Natural o Persona Jurídica (Pública o Privada) que tiene relación de dependencia.	NO		OID 2.5.4.11
1.6.5. Organization Identifier	Número de Registro Unico de Contribuyente de la persona jurídica (Pública o Privada) a la que está vinculado el Signatario "VAT(CÓDIGO_PAÍS)-RUC" Ej. VATEC-1716151413001	NO		OID 2.5.4.97 codificación acorde la ETSI EN 319 412-1 RFC 5280 establece como no obligatorio
1.6.6. Title	Se especificará el nombre del título o el puesto (cargo) que el Signatario ocupa	NO		OID 2.5.4.12
1.6.7. Surname	Apellidos del Signatario (como consta en el documento oficial)	SI		OID 2.5.4.4
1.6.8. Given Name	Nombres del Signatario (como consta en el documento oficial)	SI		OID 2.5.4.42
1.6.9. Serial Number	Número de cédula (IDC"País"-1716151413) o pasaporte (PAS"País"-A6362611) del signatario Ej. IDCEC-1716151413 o PASEC-A6362611	SI		OID 2.5.4.5 Número de documento oficial codificado acorde a ETSI EN 319 412-1
1.6.10. Common Name (CN)	Nombres y Apellidos del Signatario	SI		OID 2.5.4.3
1.7. Subject Public Key Info		SI		
1.7.1. AlgorithmIdentifier				
1.7.1.1. Algorithm	RSA encryption	SI		OID 1.2.840.113549.1.1.1
1.7.1.2. Parameters	No aplicable	NO		
1.7.2. SubjectPublicKey	Clave pública del Signatario	SI		Acorde ETSI TS 119 312
2. Extensions				

 Certificamos Información Digital	PERFILES DE CERTIFICADOS DICERT		
	Revisado: Galo Becerra - GG	Código: PCD-DC-GG-014	
		Versión: 2.0	
		Clasificación de Información: DOCUMENTO CONFIDENCIAL	

2.1. Authority Key Identifier	Identificador de la clave del Issuer	NO	NO	OID 2.5.29.35 (Marcado como NO crítico según EN 319412-2) No es obligatorio siempre y cuando la clave pública de la AC se distribuya en forma de certificado "AUTOFIRMADO"
2.1.1. KeyIdentifier		NO		Derivado de la clave pública
2.2. Subject Key Identifier	Identificador de la clave del Subject	SI	NO	OID 2.5.29.14 (Marcado como NO crítico según EN 319412-2)
2.2.1. KeyIdentifier		SI		Derivado de la clave pública
2.3. Key Usage		SI	SI	OID 2.5.29.15
2.3.1. Digital Signature	Seleccionado "1"	SI		
2.3.2. Content commitment	Seleccionado "1"	SI		
2.3.3. Key Encipherment	Seleccionado "1"	SI		
2.3.4. Data Encipherment	No seleccionado. "0"			
2.3.5. Key Agreement	No seleccionado. "0"			
2.3.6. Key Certificate Signature	No seleccionado. "0"			
2.3.7. CRL Signature	No seleccionado. "0"			
2.3.8. Encipher Only	No seleccionado. "0"			
2.3.9. Decipher Only	No seleccionado. "0"			
2.4. Certificate Policies		SI	NO	OID 2.5.29.32 (Marcado como NO crítico según EN 319412-2)
2.4.1. Policy Information		SI		
2.4.1.1. Policy Identifier	1.3.6.1.4.1.oid_AC.2.6.1	SI		Identificador de la política de la AC
2.4.1.2. Policy Qualifiers		SI		
2.4.1.1.1 CPS URI	https://dicert.com.ec/links/dpc	SI		OID 1.3.6.1.5.5.7.2.1 URL de la Política de Certificados de la Entidad Acreditada
2.4.1.1.2. User Notice/Explicit text	"CERTIFICADO DE MIEMBRO DE EMPRESA O EN RELACION DE DEPENDENCIA EN ARCHIVO"	SI		OID 1.3.6.1.5.5.7.2.2 Texto indicativo
2.5. Subject Alternative Names		NO	NO	OID 2.5.29.17 (Marcado como NO crítico según EN 319412-2)

 Certificamos Información Digital	PERFILES DE CERTIFICADOS DICERT		
	Revisado: Galo Becerra - GG	Código: PCD-DC-GG-014	
		Versión: 2.0	
		Clasificación de Información: DOCUMENTO CONFIDENCIAL	

2.5.1. rfc822Name	Correo electrónico del Titular de la Firma nombreaapellido@example.com.ec	SI		
2.6. Extended Key Usage		SI	NO	OID 2.5.29.37 (Marcado como NO crítico según EN 319412-2)
2.6.1. clientAuth	Presente (1.3.6.1.5.5.7.3.2)	SI		Transport Layer Security (TLS) World Wide Web (WWW) client authentication
2.6.2. Email protection	Presente (1.3.6.1.5.5.7.3.4)	SI		Sí se incluye el correo electrónico del Signatario
2.7. cRLDistributionPoint		NO	NO	OID 2.5.29.31 (Marcado como NO crítico según EN 319412-2)
2.7.1. distributionPoint	https://dicert.com.ec/links/crl1	SI		http (http://) IETF RFC 7230-7235 [3] or ldap (ldap://) IETF RFC 4516 [4] scheme
2.7.2. distributionPoint	https://dicert.com.ec/links/crl2	NO		http (http://) IETF RFC 7230-7235 [3] or ldap (ldap://) IETF RFC 4516 [4] scheme
2.8. Authority Information Access		SI	NO	OID 1.3.6.1.5.5.7.1.1 (Marcado como NO crítico según EN 319412-2)
2.8.1. Access Description		SI		
2.8.1.1. Access Method	id-ad-ocsp	SI		OID 1.3.6.1.5.5.7.48.1
2.8.1.1.1 Access Location	https://dicert.com.ec/links/ocsp	SI		URL de acceso al OCSP (http://) IETF RFC 7230-7235 [3] or https (https://) IETF RFC 2818 [5]
2.8.1.1.2 Access Location		NO		URL de acceso al OCSP (http://) IETF RFC 7230-7235 [3] or https (https://) IETF RFC 2818 [5]
2.8.2. Access Description		NO		No es obligatorio siempre y cuando incluya la ubicación de acceso al OCSP
2.8.2.1. Access Method	id-ad-calssuers	NO		OID 1.3.6.1.5.5.7.48.2
2.8.2.1.1 Access Location	https://dicert.com.ec/links/certac	NO		URL acceso a certificado de la AC (http://) IETF RFC 7230-7235 [3] or https (https://) IETF RFC 2818 [5]
2.9. Basic Constraints		SI	SI	OID 2.5.29.19
2.9.1. cA	FALSE	SI		

	PERFILES DE CERTIFICADOS DICERT		
	Revisado: Galo Becerra - GG	Código: PCD-DC-GG-014	
		Versión: 2.0	
		Clasificación de Información: DOCUMENTO CONFIDENCIAL	

3. Perfil Certificado de Representante Legal en Archivo

REPRESENTANTE LEGAL EN ARCHIVO - ANEXO 3A				
Campo	En Archivo	Obligatorio	Crítico	Observaciones 1.3.6.1.4.1.62486.2.3.1
De Representante Legal	Autenticación y Firma			
1. Basic structure				
1.1. Version	"2"	SI		El literal “2” corresponde a la versión 3. X.509
1.2. Serial Number	Establecido automáticamente por la AC Número identificativo único del certificado.	SI		No puede ser un número negativo ni 0.
1.3. Signature Algorithm		SI		
1.3.1. Algorithm	SHA-256 with RSA Signature	SI		1.2.840.113549.1.1.11
1.3.2. Parameters	No aplicable	NO		
1.4. Issuer		SI		
1.4.1. Country Name (C)	Código del País "EC" (ISO 3166)	SI		OID 2.5.4.6
1.4.2. Organization Name (O)	DICERT S.A.	SI		OID 2.5.4.10
1.4.3. Locality Name (L)	QUITO	SI		OID 2.5.4.7
1.4.4. Organization Identifier	VATEC-1793151884001	NO		OID 2.5.4.97 codificación acorde la ETSI EN 319 412-1 RFC 5280 establece como no obligatorio
1.4.5. Common Name (CN)	Nombre de la AC Subordinada "DICERT AC SUBORDINADA"	SI		OID 2.5.4.3
1.4.6. Organizational Unit Name (OU)	UNIDAD DE CERTIFICACION ELECTRONICA	NO		OID 2.5.4.11
1.5. Validity		SI		
1.5.1. Not Before	Fecha de inicio de validez	SI		YYMMDDHHMMSSZ
1.5.2. Not After	Fecha de expiración	SI		YYMMDDHHMMSSZ
1.6. Subject		SI		
1.6.1. Country Name (C)	País donde reside de la Persona Jurídica (Pública o Privada) "EC" (ISO 3166)	SI		OID 2.5.4.6

 Certificamos Información Digital	PERFILES DE CERTIFICADOS DICERT		
	Revisado: Galo Becerra - GG	Código: PCD-DC-GG-014	
		Versión: 2.0	
		Clasificación de Información: DOCUMENTO CONFIDENCIAL	

1.6.2. Locality Name (L)	Localidad de la Persona Jurídica (Ciudad) ej. QUITO	SI		OID 2.5.4.7
1.6.3. Organization Name (O)	Persona Jurídica (Pública o Privada) de la cual es Representante Legal o Apoderado el Signatario	SI		OID 2.5.4.10
1.6.4. Organization Identifier	Número de Registro Unico de Contribuyente de la persona jurídica (Pública o Privada) a la que está vinculado el Signatario "VAT(CÓDIGO_PAÍS)-RUC" Ej. VATEC-1716151413001	NO		OID 2.5.4.97 codificación acorde la ETSI EN 319 412-1 RFC 5280 establece como no obligatorio
1.6.5. Title	Se especificará el nombre del título o el puesto (cargo) que el Signatario ocupa	NO		OID 2.5.4.12
1.6.6. Surname	Apellidos del Signatario (como consta en el documento oficial)	SI		OID 2.5.4.4
1.6.7. Given Name	Nombres del Signatario (como consta en el documento oficial)	SI		OID 2.5.4.42
1.6.8. Serial Number	Número de cédula (IDC"País"-1716151413) o pasaporte (PAS"País"-A6362611) del Signatario Ej. IDCEC-1716151413 o PASEC-A6362611	SI		OID 2.5.4.5 Número de documento oficial codificado acorde a ETSI EN 319 412-1
1.6.9. Common Name (CN)	Nombres y Apellidos del Signatario	SI		OID 2.5.4.3
1.7. Subject Public Key Info		SI		
1.7.1. AlgorithmIdentifier				
1.7.1.1. Algorithm	RSA encryption	SI		OID 1.2.840.113549.1.1.1
1.7.1.2. Parameters	No aplicable	NO		
1.7.2. SubjectPublicKey	Clave pública del Signatario	SI		Acorde ETSI TS 119 312
2. Extensions				
2.1. Authority Key Identifier	Identificador de la clave del Issuer	NO	NO	OID 2.5.29.35 (Marcado como NO crítico según EN 319412-2) No es obligatorio siempre y cuando la clave pública de la AC se distribuya en forma de certificado "AUTOFIRMADO"
2.1.1. KeyIdentifier		NO		Derivado de la clave pública
2.2. Subject Key Identifier	Identificador de la clave del Subject	SI	NO	OID 2.5.29.14 (Marcado como NO crítico según EN 319412-2)

 Certificamos Información Digital	PERFILES DE CERTIFICADOS DICERT		
	Revisado: Galo Becerra - GG	Código: PCD-DC-GG-014	
		Versión: 2.0	
		Clasificación de Información: DOCUMENTO CONFIDENCIAL	

2.2.1. KeyIdentifier		SI		Derivado de la clave pública
2.3. Key Usage		SI	SI	OID 2.5.29.15
2.3.1. Digital Signature	Seleccionado "1"	SI		
2.3.2. Content commitment	Seleccionado "1"	SI		
2.3.3. Key Encipherment	Seleccionado "1"	SI		
2.3.4. Data Encipherment	No seleccionado. "0"			
2.3.5. Key Agreement	No seleccionado. "0"			
2.3.6. Key Certificate Signature	No seleccionado. "0"			
2.3.7. CRL Signature	No seleccionado. "0"			
2.3.8. Encipher Only	No seleccionado. "0"			
2.3.9. Decipher Only	No seleccionado. "0"			
2.4. Certificate Policies		SI	NO	OID 2.5.29.32 (Marcado como NO crítico según EN 319412-2)
2.4.1. Policy Information		SI		
2.4.1.1. Policy Identifier	1.3.6.1.4.1.oid_AC.2.6.1	SI		Identificador de la política de la AC
2.4.1.2. Policy Qualifiers		SI		
2.4.1.1.1 CPS URI	https://dicert.com.ec/links/dpc	SI		OID 1.3.6.1.5.5.7.2.1 URL de la Política de Certificados de la Entidad Acreditada
2.4.1.1.2. User Notice/Explicit text	"CERTIFICADO DE REPRESENTANTE LEGAL EN ARCHIVO"	SI		OID 1.3.6.1.5.5.7.2.2 Texto indicativo
2.5. Subject Alternative Names		NO	NO	OID 2.5.29.17 (Marcado como NO crítico según EN 319412-2)
2.5.1. rfc822Name	Correo electrónico del Titular de la Firma nombreapellido@example.com.ec	SI		
2.6. Extended Key Usage		SI	NO	OID 2.5.29.37 (Marcado como NO crítico según EN 319412-2)
2.6.1. clientAuth	Presente (1.3.6.1.5.5.7.3.2)	SI		Transport Layer Security (TLS) World Wide Web (WWW) client authentication
2.6.2. Email protection	Presente (1.3.6.1.5.5.7.3.4)	SI		Sí se incluye el correo electrónico del Signatario

 Certificamos Información Digital	PERFILES DE CERTIFICADOS DICERT			
	Revisado: Galo Becerra - GG	Código: PCD-DC-GG-014		
		Versión: 2.0		
		Clasificación de Información: DOCUMENTO CONFIDENCIAL		

2.7. cRLDistributionPoint		NO	NO	OID 2.5.29.31 (Marcado como NO crítico según EN 319412-2)
2.7.1. distributionPoint	https://dicert.com.ec/links/crl1	SI		http (http://) IETF RFC 7230-7235 [3] or ldap (ldap://) IETF RFC 4516 [4] scheme
2.7.2. distributionPoint	https://dicert.com.ec/links/crl2	NO		http (http://) IETF RFC 7230-7235 [3] or ldap (ldap://) IETF RFC 4516 [4] scheme
2.8. Authority Information Access		SI	NO	OID 1.3.6.1.5.5.7.1.1 (Marcado como NO crítico según EN 319412-2)
2.8.1. Access Description		SI		
2.8.1.1. Access Method	id-ad-ocsp	SI		OID 1.3.6.1.5.5.7.48.1
2.8.1.1.1 Access Location	https://dicert.com.ec/links/ocsp	SI		URL de acceso al OCSP (http://) IETF RFC 7230-7235 [3] or https (https://) IETF RFC 2818 [5]
2.8.1.1.2 Access Location		NO		URL de acceso al OCSP (http://) IETF RFC 7230-7235 [3] or https (https://) IETF RFC 2818 [5]
2.8.2. Access Description		NO		No es obligatorio siempre y cuando incluya la ubicación de acceso al OCSP
2.8.2.1. Access Method	id-ad-calssuers	NO		OID 1.3.6.1.5.5.7.48.2
2.8.2.1.1 Access Location	https://dicert.com.ec/links/certac	NO		URL acceso a certificado de la AC (http://) IETF RFC 7230-7235 [3] or https (https://) IETF RFC 2818 [5]
2.9. Basic Constraints		SI	SI	OID 2.5.29.19
2.9.1. cA	FALSE	SI		

4. Perfil Certificado de Sello Electrónico en Archivo

SELLO ELECTRÓNICO EN ARCHIVO - ANEXO 4A				
Campo	En Archivo	Obligatorio	Crítico	Observaciones 1.3.6.1.4.1.62486.2.4.1
Cert SELLO ELECTRÓNICO	Autenticación y Firma			

 Certificamos Información Digital	PERFILES DE CERTIFICADOS DICERT		
	Revisado: Galo Becerra - GG	Código: PCD-DC-GG-014	
		Versión: 2.0	
		Clasificación de Información: DOCUMENTO CONFIDENCIAL	

1. Basic estructura				
1.1. Version	"2"	SI		El literal "2" corresponde a la versión 3. X.509
1.2. Serial Number	Establecido automáticamente por la AC Número identificativo único del certificado.	SI		No puede ser un número negativo ni 0.
1.3. Signature Algorithm		SI		
1.3.1. Algorithm	SHA-256 with RSA Signature	SI		1.2.840.113549.1.1.11
1.3.2. Parameters	No aplicable	NO		
1.4. Issuer		SI		
1.4.1. Country Name (C)	Código del País "EC" (ISO 3166)	SI		OID 2.5.4.6
1.4.2. Organization Name (O)	DICERT S.A.	SI		OID 2.5.4.10
1.4.3. Locality Name (L)	QUITO	SI		OID 2.5.4.7
1.4.4. Organization Identifier	VATEC-1793151884001	NO		OID 2.5.4.97 codificación acorde la ETSI EN 319 412-1 RFC 5280 establece como no obligatorio
1.4.5. Common Name (CN)	Nombre de la AC Subordinada "DICERT AC SUBORDINADA"	SI		OID 2.5.4.3
1.4.6. Organizational Unit Name (OU)	UNIDAD DE CERTIFICACION ELECTRONICA	NO		OID 2.5.4.11
1.5. Validity		SI		
1.5.1. Not Before	Fecha de inicio de validez	SI		YYMMDDHHMMSSZ
1.5.2. Not After	Fecha de expiración	SI		YYMMDDHHMMSSZ
1.6. Subject		SI		
1.6.1. Country Name (C)	País donde se encuentra registrada la Persona Jurídica (Pública o Privada) Titular de la Firma "EC" (ISO 3166)	SI		OID 2.5.4.6
1.6.2. Locality Name (L)	Localidad de la Persona Jurídica (Ciudad) ej. QUITO	SI		OID 2.5.4.7
1.6.3. Organization Name (O)	Nombre de la Persona Jurídica (Pública o Privada) Titular de la Firma Ej. "CORPORACIÓN FAVORITA"	SI		OID 2.5.4.10
1.6.4. Organizational Unit Name (OU)	Se especificará el Departamento o Área a la que pertenece el Signatario	NO		OID 2.5.4.11

 Certificamos Información Digital	PERFILES DE CERTIFICADOS DICERT		
	Revisado: Galo Becerra - GG	Código: PCD-DC-GG-014	
		Versión: 2.0	
		Clasificación de Información: DOCUMENTO CONFIDENCIAL	

1.6.5. Organization Identifier	Número de Registro Unico de Contribuyente de la persona jurídica (Pública o Privada) a la que está vinculado el Signatario "VAT(CÓDIGO_PAÍS)-RUC" Ej. VATEC-1716151413001	NO		OID 2.5.4.97 codificación acorde la ETSI EN 319 412-1 RFC 5280 establece como no obligatorio
1.6.6. Serial Number	Número de Registro Unico de Contribuyente de la Persona Jurídica (Pública o Privada) Ej."1716151413001"	SI		OID 2.5.4.5
1.6.7. Common Name (CN)	Descripción del uso que se le dará al sello electrónico. Ej. RECEPCIÓN DE DOCUMENTOS EN VENTANILLA UNICA	SI		OID 2.5.4.3
1.6.8. Surname	Apellidos del Signatario que estará vinculado el sello (como consta en el documento oficial)	SI		OID 2.5.4.4
1.6.9. Given Name	Nombres del Signatario que estará vinculado el sello (como consta en el documento oficial)	SI		OID 2.5.4.42
1.7. Subject Public Key Info		SI		
1.7.1. AlgorithmIdentifier				
1.7.1.1. Algorithm	RSA encryption	SI		OID 1.2.840.113549.1.1.1
1.7.1.2. Parameters	No aplicable	NO		
1.7.2. SubjectPublicKey	Clave pública del Signatario	SI		Acorde ETSI TS 119 312
2. Extensions				
2.1. Authority Key Identifier	Identificador de la clave del Issuer	NO	NO	OID 2.5.29.35 (Marcado como NO crítico según EN 319412-2) No es obligatorio siempre y cuando la clave pública de la AC se distribuya en forma de certificado "AUTOFIRMADO"
2.1.1. KeyIdentifier		NO		Derivado de la clave pública
2.2. Subject Key Identifier	Identificador de la clave del Subject	SI	NO	OID 2.5.29.14 (Marcado como NO crítico según EN 319412-2)
2.2.1. KeyIdentifier		SI		Derivado de la clave pública
2.3. Key Usage		SI	SI	OID 2.5.29.15
2.3.1. Digital Signature	Seleccionado "1"	SI		
2.3.2. Content commitment	Seleccionado "1"	SI		

 Certificamos Información Digital	PERFILES DE CERTIFICADOS DICERT		
	Revisado: Galo Becerra - GG	Código: PCD-DC-GG-014	
		Versión: 2.0	
		Clasificación de Información: DOCUMENTO CONFIDENCIAL	

2.3.3. Key Encipherment	Seleccionado "1"	SI		
2.3.4. Data Encipherment	No seleccionado. "0"			
2.3.5. Key Agreement	No seleccionado. "0"			
2.3.6. Key Certificate Signature	No seleccionado. "0"			
2.3.7. CRL Signature	No seleccionado. "0"			
2.3.8. Encipher Only	No seleccionado. "0"			
2.3.9. Decipher Only	No seleccionado. "0"			
2.4. Certificate Policies		SI	NO	OID 2.5.29.32 (Marcado como NO crítico según EN 319412-2)
2.4.1. Policy Information		SI		
2.4.1.1. Policy Identifier	1.3.6.1.4.1.oid_AC.2.6.1	SI		Identificador de la política de la AC
2.4.1.2. Policy Qualifiers		SI		
2.4.1.1.1 CPS URI	https://dicert.com.ec/links/dpc	SI		OID 1.3.6.1.5.5.7.2.1 URL de la Política de Certificados de la Entidad Acreditada
2.4.1.1.2. User Notice/Explicit text	"CERTIFICADO DE SELLO ELECTRÓNICO EN ARCHIVO"	SI		OID 1.3.6.1.5.5.7.2.2 Texto indicativo
2.5. Subject Alternative Names		NO	NO	OID 2.5.29.17 (Marcado como NO crítico según EN 319412-2)
2.5.1. rfc822Name	Correo electrónico de la Persona Jurídica (Pública o Privada) Titular de la Firma (sello electrónico) "info@example.com.ec"	SI		
2.6. Extended Key Usage		SI	NO	OID 2.5.29.37 (Marcado como NO crítico según EN 319412-2)
2.6.1. clientAuth	Presente (1.3.6.1.5.5.7.3.2)	SI		Transport Layer Security (TLS) World Wide Web (WWW) client authentication
2.6.2. Email protection	Presente (1.3.6.1.5.5.7.3.4)	SI		Sí se incluye el correo electrónico de la Persona Jurídica
2.7. cRLDistributionPoint		NO	NO	OID 2.5.29.31 (Marcado como NO crítico según EN 319412-2)
2.7.1. distributionPoint	https://dicert.com.ec/links/crl1	SI		http (http://) IETF RFC 7230-7235 [3] or ldap (ldap://) IETF RFC 4516 [4] scheme

 Certificamos Información Digital	PERFILES DE CERTIFICADOS DICERT			
	Revisado: Galo Becerra - GG			Código: PCD-DC-GG-014
				Versión: 2.0
				Clasificación de Información: DOCUMENTO CONFIDENCIAL

2.7.2. distributionPoint	https://dicert.com.ec/links/crl2	NO		http (http://) IETF RFC 7230-7235 [3] or ldap (ldap://) IETF RFC 4516 [4] scheme
2.8. Authority Information Access		SI	NO	OID 1.3.6.1.5.5.7.1.1 (Marcado como NO crítico según EN 319412-2)
2.8.1. Access Description		SI		
2.8.1.1. Access Method	id-ad-ocsp	SI		OID 1.3.6.1.5.5.7.48.1
2.8.1.1.1 Access Location	https://dicert.com.ec/links/ocsp	SI		URL de acceso al OCSP (http://) IETF RFC 7230-7235 [3] or https (https://) IETF RFC 2818 [5]
2.8.1.1.2 Access Location		NO		URL de acceso al OCSP (http://) IETF RFC 7230-7235 [3] or https (https://) IETF RFC 2818 [5]
2.8.2. Access Description		NO		No es obligatorio siempre y cuando incluya la ubicación de acceso al OCSP
2.8.2.1. Access Method	id-ad-calssuers	NO		OID 1.3.6.1.5.5.7.48.2
2.8.2.1.1 Access Location	https://dicert.com.ec/links/certac	NO		URL acceso a certificado de la AC (http://) IETF RFC 7230-7235 [3] or https (https://) IETF RFC 2818 [5]
2.9. Basic Constraints		SI	SI	OID 2.5.29.19
2.9.1. cA	FALSE	SI		

5. Perfil Certificado de Sellado de Tiempo

SELLADO DE TIEMPO - ANEXO 5				
Campo		Obligatorio	Crítico	Observaciones 1.3.6.1.4.1.62486.2.5.1
Cert Sellado de Tiempo	Autenticación y Firma			
1. Basic structure				
1.1. Version	"2"	SI		El literal "2" corresponde a la versión 3. X.509
1.2. Serial Number	Establecido automáticamente por la AC Número identificativo único del certificado.	SI		No puede ser un número negativo ni 0.

 Certificamos Información Digital	PERFILES DE CERTIFICADOS DICERT		
	Revisado: Galo Becerra - GG	Código: PCD-DC-GG-014	
		Versión: 2.0	
		Clasificación de Información: DOCUMENTO CONFIDENCIAL	

1.3. Signature Algorithm		SI		
1.3.1. Algorithm	SHA-256 with RSA Signature	SI		1.2.840.113549.1.1.11
1.3.2. Parameters	No aplicable	NO		
1.4. Issuer		SI		
1.4.1. Country Name (C)	Código del País "EC" (ISO 3166)	SI		OID 2.5.4.6
1.4.2. Locality Name (L)	QUITO	SI		OID 2.5.4.7
1.4.3. Organization Name (O)	DICERT S.A.	SI		OID 2.5.4.10
1.4.4. Organization Identifier	VATEC-1793151884001	NO		OID 2.5.4.97 codificación acorde la ETSI EN 319 412-1 RFC 5280 establece como no obligatorio
1.4.5. Common Name (CN)	Nombre de la AC Subordinada "DICERT AC SUBORDINADA"	SI		OID 2.5.4.3
1.4.6. Organizational Unit (OU)	UNIDAD DE CERTIFICACION ELECTRONICA	NO		OID 2.5.4.11
1.5. Validity		SI		
1.5.1. Not Before	Fecha de inicio de validez	SI		YYMMDDHHMMSSZ
1.5.2. Not After	Fecha de expiración	SI		YYMMDDHHMMSSZ
1.6. Subject		SI		
1.6.1. Country Name (C)	País donde se encuentra registrada la Persona Jurídica (Pública o Privada) Titular de la Firma "EC" (ISO 3166)	SI		OID 2.5.4.6
1.6.2. Organization Name (O)	Nombre de la Persona Jurídica (Pública o Privada) Titular de la Firma solicitante del sellado de tiempo ej. "NOTARIA"	SI		OID 2.5.4.10
1.6.3. Locality Name (L)	Localidad de la Persona Jurídica (Pública o Privada) (Ciudad) ej. QUITO	SI		OID 2.5.4.7
1.6.4. Organization Identifier	Número de Registro Unico de Contribuyente de la persona jurídica (Pública o Privada) a la que está vinculado el Sellado de Tiempo "VAT(CÓDIGO_PAÍS)-RUC" Ej. VATEC-1716151413001	NO		OID 2.5.4.97 codificación acorde la ETSI EN 319 412-1 RFC 5280 establece como no obligatorio
1.6.5. Serial Number	Número de Registro Unico de Contribuyente de la Persona Jurídica (Pública o Privada)	SI		OID 2.5.4.5

 Certificamos Información Digital	PERFILES DE CERTIFICADOS DICERT		
	Revisado: Galo Becerra - GG	Código: PCD-DC-GG-014	
		Versión: 2.0	
		Clasificación de Información: DOCUMENTO CONFIDENCIAL	

	Ej."1716151413001"			
1.6.6. Common Name (CN)	Nombre del Servicio "Sellado de tiempo de la Persona Jurídica (Pública o Privada)"	SI		OID 2.5.4.3
1.6.7. Organizational Unit (OU)	Nombre de la Unidad Organizativa de la Persona Jurídica (Pública o Privada) Ej. UNIDAD DE SELLADO DE TIEMPO DE LA NOTARIA	SI		OID 2.5.4.11
1.7. Subject Public Key Info		SI		
1.7.1. AlgorithmIdentifier				
1.7.1.1. Algorithm	RSA encryption	SI		OID 1.2.840.113549.1.1.1
1.7.1.2. Parameters	No aplicable	NO		
1.7.2. SubjectPublicKey	Clave pública codificada de acuerdo con el algoritmo criptográfico. 2048 bits	SI		Acorde ETSI TS 119 312
2. Extensions				
2.1. Authority Key Identifier	Identificador de la clave del Issuer	NO	NO	OID 2.5.29.35 (Marcado como NO crítico según EN 319412-2) No es obligatorio siempre y cuando la clave pública de la AC se distribuya en forma de certificado "AUTOFIRMADO"
2.1.1. KeyIdentifier		NO		Derivado de la clave pública
2.2. Subject Key Identifier	Identificador de la clave del Subject	SI	NO	OID 2.5.29.14 (Marcado como NO crítico según EN 319412-2)
2.2.1. KeyIdentifier		SI		Derivado de la clave pública
2.3. Key Usage		SI	SI	OID 2.5.29.15
2.3.1. Digital Signature	Seleccionado "1"	SI		
2.3.2. Content commitment	No seleccionado. "0"			
2.3.3. Key Encipherment	No seleccionado. "0"			
2.3.4. Data Encipherment	No seleccionado. "0"			
2.3.5. Key Agreement	No seleccionado. "0"			
2.3.6. Key Certificate Signature	No seleccionado. "0"			
2.3.7. CRL Signature	No seleccionado. "0"			
2.3.8. Encipher Only	No seleccionado. "0"			
2.3.9. Decipher Only	No seleccionado. "0"			

 Certificamos Información Digital	PERFILES DE CERTIFICADOS DICERT		
	Revisado: Galo Becerra - GG	Código: PCD-DC-GG-014	
		Versión: 2.0	
		Clasificación de Información: DOCUMENTO CONFIDENCIAL	

2.4. Certificate Policies		SI	NO	OID 2.5.29.32 (Marcado como NO crítico según EN 319412-2)
2.4.1. Policy Information		SI		
2.4.1.1. Policy Identifier	1.3.6.1.4.1.oid_AC.2.6.1	SI		Identificador de la política de la AC
2.4.1.2. Policy Qualifiers		SI		
2.4.1.1.1 CPS URI	https://dicert.com.ec/links/dpc	SI		OID 1.3.6.1.5.5.7.2.1 URL de la Política de Certificados de la Entidad Acreditada
2.4.1.1.2. User Notice/Explicit text	"CERTIFICADO DE SELLADO DE TIEMPO"	SI		OID 1.3.6.1.5.5.7.2.2 Texto indicativo
2.5. Subject Alternative Names		SI	NO	OID 2.5.29.17 (Marcado como NO crítico según EN 319412-2)
2.5.1. rfc822Name	Correo electrónico de la Persona Jurídica (Pública o Privada) Titular de la Firma "info@example.com.ec"	SI		
2.6. Extended Key Usage		SI	SI	OID 2.5.29.37 (Marcado como crítico según RFC 3161)
2.6.1. TimeStamping	Presente (1.3.6.1.5.5.7.3.8)	SI		
2.7. cRLDistributionPoint		NO	NO	OID 2.5.29.31 (Marcado como NO crítico según EN 319412-2)
2.7.1. distributionPoint	https://dicert.com.ec/links/crl1	SI		http (http://) IETF RFC 7230-7235 [3] or ldap (ldap://) IETF RFC 4516 [4] scheme
2.7.2. distributionPoint	https://dicert.com.ec/links/crl2	NO		http (http://) IETF RFC 7230-7235 [3] or ldap (ldap://) IETF RFC 4516 [4] scheme
2.8. Authority Information Access		SI	NO	OID 1.3.6.1.5.5.7.1.1 (Marcado como NO crítico según EN 319412-2)
2.8.1. Access Description		SI		
2.8.1.1. Access Method	id-ad-ocsp	SI		OID 1.3.6.1.5.5.7.48.1
2.8.1.1.1 Access Location	https://dicert.com.ec/links/oscp	SI		URL de acceso al OCSP (http://) IETF RFC 7230-7235 [3] or https (https://) IETF RFC 2818 [5]

 Certificamos Información Digital	PERFILES DE CERTIFICADOS DICERT		
	Revisado: Galo Becerra - GG	Código: PCD-DC-GG-014	
		Versión: 2.0	
		Clasificación de Información: DOCUMENTO CONFIDENCIAL	

2.8.1.1.2 Access Location		NO		URL de acceso al OCSP (http://) IETF RFC 7230-7235 [3] or https (https://) IETF RFC 2818 [5]
2.8.2. Access Description		NO		No es obligatorio siempre y cuando incluya la ubicación de acceso al OCSP
2.8.2.1. Access Method	id-ad-calssuers	NO		OID 1.3.6.1.5.5.7.48.2
2.8.2.1.1 Access Location	https://dicert.com.ec/links/certac	NO		URL acceso a certificado de la AC (http://) IETF RFC 7230-7235 [3] or https (https://) IETF RFC 2818 [5]
2.9. Basic Constraints		SI	SI	OID 2.5.29.19
2.9.1. cA	FALSE	SI		

6. Perfil Certificado de Certificado Raíz | AC Root

CERTIFICADO RAIZ - AC (ROOT) - ANEXO 6				
Campo	Contenido	Obligatorio	Crítico	Observaciones 1.3.6.1.4.1.62486.n
1. Basic structure				
1.1. Version	"2"	SI		El literal "2" corresponde a la versión 3. X.509
1.2. Serial Number	Establecido automáticamente por la AC Número identificativo único del certificado.	SI		No puede ser un número negativo ni 0.
1.3. Signature Algorithm		SI		
1.3.1. Identifier	1.2.840.113549.1.1.11	SI		1.2.840.113549.1.1.11
1.3.2. Description	SHA-256 with RSA Signature	SI		
1.4. Issuer		SI		
1.4.1. Common Name (CN)	DICERT ROOT CA	SI		OID 2.5.4.3
1.4.2. Country (C)	Código del País "EC" (ISO 3166)	SI		OID 2.5.4.6
1.4.3. Organization Name (O)	Nombre de la AC Rapiz "DICERT S.A."	SI		OID 2.5.4.10
1.4.4. Locality (L)	Localidad de la AC Raíz. "QUITO"	SI		OID 2.5.4.7
1.4.5. Organizational Unit (OU)	Nombre de la Unidad Organizativa de las AC Raíz. "UNIDAD DE CERTIFICACION ELECTRONICA"	NO		OID 2.5.4.11

 Certificamos Información Digital	PERFILES DE CERTIFICADOS DICERT		
	Revisado: Galo Becerra - GG	Código: PCD-DC-GG-014	
		Versión: 2.0	
		Clasificación de Información: DOCUMENTO CONFIDENCIAL	

1.4.6. Organization Identifier	VATEC-1793151884001	NO		OID 2.5.4.97 codificación acorde la ETSI EN 319 412-1 RFC 5280 establece como no obligatorio
1.5. Validity		SI		
1.5.1. Not Before	Fecha de inicio de validez	SI		YYMMDDHHMMSSZ
1.5.2. Not After	Fecha de expiración	SI		YYMMDDHHMMSSZ
1.6. Subject	Mismos datos entre Issuer y Subject (Autofirmado)	SI		
1.6.1. Common Name (CN)	DICERT ROOT CA	SI		OID 2.5.4.3
1.6.2. Country (C)	EC	SI		OID 2.5.4.6
1.6.3. Organization Name (O)	DICERT S.A.	SI		OID 2.5.4.10
1.6.4. Locality (L)	QUITO	SI		OID 2.5.4.7
1.6.5. Organizational Unit (OU)	UNIDAD DE CERTIFICACION ELECTRONICA	NO		OID 2.5.4.11
1.6.6. Organization Identifier	VATEC-1793151884001	NO		OID 2.5.4.97 codificación acorde la ETSI EN 319 412-1 RFC 5280 establece como no obligatorio
1.7. Subject Public Key Info	Clave pública de la AC Raíz, codificada de acuerdo con el algoritmo criptográfico.	SI		
1.7.1. AlgorithmIdentifier	1.2.840.113549.1.1.1			
1.7.1.1. Algorithm	RSA encryption	SI		OID 1.2.840.113549.1.1.1
1.7.1.2. Parameters	No aplicable	NO		
1.7.2. SubjectPublicKey	Clave pública codificada de acuerdo con el algoritmo criptográfico. 4096 bits	SI		Acorde ETSI TS 119 312
2. Extensions				
2.1. Authority Key Identifier	Presente	NO	NO	OID 2.5.29.35 (Marcado como NO crítico según EN 319412-2) No es obligatorio siempre y cuando la clave pública de la AC se distribuya en forma de certificado "AUTOFIRMADO"
2.1.1. KeyIdentifier	Identificador de la clave del issuer	NO		Derivado de la clave pública

	PERFILES DE CERTIFICADOS DICERT			
	Revisado: Galo Becerra - GG	Código: PCD-DC-GG-014		
		Versión: 2.0		
		Clasificación de Información: DOCUMENTO CONFIDENCIAL		

2.2. Subject Key Identifier	Presente	SI	NO	OID 2.5.29.14 (Marcado como NO crítico según EN 319412-2)
2.2.1. KeyIdentifier	Identificador de la clave del subject	SI		Derivado de la clave pública
2.3. Key Usage		SI	SI	OID 2.5.29.15
2.3.1. Digital Signature	No seleccionado. "0"			
2.3.2. Content commitment	No seleccionado. "0"			
2.3.3. Key Encipherment	No seleccionado. "0"			
2.3.4. Data Encipherment	No seleccionado. "0"			
2.3.5. Key Agreement	No seleccionado. "0"			
2.3.6. Key Certificate Signature	Seleccionado "1"	SI		
2.3.7. CRL Signature	Seleccionado "1"	SI		
2.4. Certificate Policies	Políticas de certificación / DPC	SI	NO	OID 2.5.29.32 (Marcado como NO crítico según EN 319412-2)
2.4.1. Policy Information		SI		
2.4.1.1. Policy Identifier	1.3.6.1.4.1.oid_AC.2.6.1	SI		Identificador de la política
2.4.1.2. Policy Qualifiers	Especificación de la DPC	SI		
2.4.1.2.1 CPS URI	https://dicert.com.ec/links/dpc	SI		
2.4.1.2.2. User Notice	https://www.dicert.com.ec/legaldocs	SI		
2.5. Subject Alternative Names			NO	
2.5.1. rfc822Name	soporte@dicert.com.ec	SI		
2.6. Basic Constraints		SI	SI	OID 2.5.29.19
2.6.1. Subject type	ca (TRUE)	SI		
2.6.2. Path Length Constraints	0	SI		

7. Perfil Certificado de Certificado Subordinado | AC Sub

CERTIFICADO SUBORDINADO - AC SUB - ANEXO 7				
Campo	Contenido	Obligatorio	Crítico	Observaciones 1.3.6.1.4.1.62486.n

 Certificamos Información Digital	PERFILES DE CERTIFICADOS DICERT		
	Revisado: Galo Becerra - GG	Código: PCD-DC-GG-014	
		Versión: 2.0	
		Clasificación de Información: DOCUMENTO CONFIDENCIAL	

1. Basic estructura				
1.1. Version	"2"	SI		El literal "2" corresponde a la versión 3. X.509
1.2. Serial Number	Establecido automáticamente por la AC Número identificativo único del certificado.	SI		No puede ser un número negativo ni 0.
1.3. Signature Algorithm		SI		
1.3.1. Identifier	1.2.840.113549.1.1.11	SI		1.2.840.113549.1.1.11
1.3.2. Description	SHA-256 with RSA Signature	SI		
1.4. Issuer		SI		
1.4.1. Common Name (CN)	DICERT ROOT CA	SI		OID 2.5.4.3
1.4.2. Country Name (C)	EC	SI		OID 2.5.4.6
1.4.3. Organization Name (O)	DICERT S.A.	SI		OID 2.5.4.10
1.4.4. Locality Name (L)	QUITO	SI		OID 2.5.4.7
1.4.5. Organizational Unit (OU)	UNIDAD DE CERTIFICACION ELECTRONICA	NO		OID 2.5.4.11
1.4.6. Organization Identifier	VATEC-1793151884001	NO		OID 2.5.4.97 codificación acorde la ETSI EN 319 412-1 RFC 5280 establece como no obligatorio
1.5. Validity		SI		
1.5.1. Not Before	Fecha de inicio de validez	SI		YYMMDDHHMMSSZ
1.5.2. Not After	Fecha de expiración	SI		YYMMDDHHMMSSZ
1.6. Subject		SI		
1.6.1. Common Name (CN)	Nombre de la AC Subordinada "DICERT AC SUBORDINADA"	SI		OID 2.5.4.3
1.6.2. Country Name (C)	EC	SI		OID 2.5.4.6
1.6.3. Organization Name (O)	DICERT S.A.	SI		OID 2.5.4.10
1.6.4. Locality Name (L)	QUITO	SI		OID 2.5.4.7
1.6.5. Organizational Unit (OU)	UNIDAD DE CERTIFICACION ELECTRONICA	NO		OID 2.5.4.11
1.6.6. Organization Identifier	VATEC-1793151884001	NO		OID 2.5.4.97 codificación acorde la ETSI EN 319 412-1 RFC 5280 establece como no obligatorio

 Certificamos Información Digital	PERFILES DE CERTIFICADOS DICERT		
	Revisado: Galo Becerra - GG	Código: PCD-DC-GG-014	
		Versión: 2.0	
		Clasificación de Información: DOCUMENTO CONFIDENCIAL	

1.7. Subject Public Key Info	Clave pública del prestador, codificada de acuerdo con el algoritmo criptográfico.	SI		
1.7.1. AlgorithmIdentifier	1.2.840.113549.1.1.1			
1.7.1.1. Algorithm	RSA encryption	SI		OID 1.2.840.113549.1.1.1
1.7.1.2. Parameters	No aplicable	NO		
1.7.2. SubjectPublicKey	Clave pública codificada de acuerdo con el algoritmo criptográfico. 4096 bits	SI		
2. Extensions				
2.1. Authority Key Identifier	Presente	NO	NO	OID 2.5.29.35 (Marcado como NO crítico según EN 319412-2) No es obligatorio siempre y cuando la clave pública de la AC se distribuya en forma de certificado "AUTOFIRMADO"
2.1.1. KeyIdentifier	Identificador de la clave del issuer	NO		
2.2. Subject Key Identifier	Presente	SI	NO	OID 2.5.29.14 (Marcado como NO crítico según EN 319412-2)
2.2.1. KeyIdentifier	Identificador de la clave del subject	SI		
2.3. Key Usage		SI	SI	OID 2.5.29.15
2.3.1. Digital Signature	No seleccionado. "0"			
2.3.2. Content commitment	No seleccionado. "0"			
2.3.3. Key Encipherment	No seleccionado. "0"			
2.3.4. Data Encipherment	No seleccionado. "0"			
2.3.5. Key Agreement	No seleccionado. "0"			
2.3.6. Key Certificate Signature	Seleccionado "1"	SI		
2.3.7. CRL Signature	Seleccionado "1"	SI		
2.4. Certificate Policies	Políticas de certificación / DPC	SI	NO	OID 2.5.29.32 (Marcado como NO crítico según EN 319412-2)
2.4.1. Policy Information		SI		
2.4.1.1. Policy Identifier	1.3.6.1.4.1.oid_AC.2.6.1	SI		Identificador de la política
2.4.1.2. Policy Qualifiers	Especificación de la DPC	SI		
2.4.1.2.1 CPS URI	https://dicert.com.ec/links/dpc	SI		
2.4.1.2.2. User Notice	https://www.dicert.com.ec/legaldoc	SI		

 Certificamos Información Digital	PERFILES DE CERTIFICADOS DICERT			
	Revisado: Galo Becerra - GG	Código: PCD-DC-GG-014		
		Versión: 2.0		
		Clasificación de Información: DOCUMENTO CONFIDENCIAL		

	is			
2.5. Subject Alternative Names		NO	NO	OID 2.5.29.17 (Marcado como NO crítico según EN 319412-2)
2.5.1. rfc822Name	soporte@dicert.com.ec	SI		
2.6. cRLDistributionPoint		SI	NO	OID 2.5.29.31 (Marcado como NO crítico según EN 319412-2)
2.6.1 distributionPoint	https://dicert.com.ec/links/crl1	SI		http (http://) IETF RFC 7230-7235 [3] or ldap (ldap://) IETF RFC 4516 [4] scheme
2.6.2 distributionPoint	https://dicert.com.ec/links/crl2	NO		http (http://) IETF RFC 7230-7235 [3] or ldap (ldap://) IETF RFC 4516 [4] scheme
2.7 Authority Information Access		NO	NO	OID 1.3.6.1.5.5.7.1.1 (Marcado como NO crítico según EN 319412-2)
2.7.1 Access Method	id-ad-ocsp	NO		OID 1.3.6.1.5.5.7.48.1
2.7.2 Access Location	https://dicert.com.ec/links/ocsp	NO		URL de acceso al OCSP (http://) IETF RFC 7230-7235 [3] or https (https://) IETF RFC 2818 [5]
2.7.3 Access Location		NO		URL de acceso al OCSP (http://) IETF RFC 7230-7235 [3] or https (https://) IETF RFC 2818 [5]
2.8. Basic Constraints		SI	SI	OID 2.5.29.19
2.8.1. Subject type	ca (TRUE)	SI		
2.8.2. Path Length Constraints	0	SI		

8. Perfil Certificado de Certificado de Validación OCSP

CERTIFICADO DE VALIDACION OCSP - ANEXO 8				
Campo	Autenticación o Firma	Obligatorio	Crítico	Observaciones 1.3.6.1.4.1.62486.2.6.1
de Certificado de Validación OCSP				

 Certificamos Información Digital	PERFILES DE CERTIFICADOS DICERT		
	Revisado: Galo Becerra - GG	Código: PCD-DC-GG-014	
		Versión: 2.0	
		Clasificación de Información: DOCUMENTO CONFIDENCIAL	

1. Basic estructura				
1.1. Version	"2"	SI		El literal "2" corresponde a la versión 3. X.509
1.2. Serial Number	Establecido automáticamente por la AC Número identificativo único del certificado.	SI		No puede ser un número negativo ni 0.
1.3. Signature Algorithm	1.2.840.113549.1.1.11	SI		
1.3.1. Algorithm	SHA-256 with RSA Signature	SI		1.2.840.113549.1.1.11
1.3.2. Parameters	No aplicable	NO		
1.4. Issuer		SI		
1.4.1. Country Name (C)	EC	SI		OID 2.5.4.6
1.4.2. Locality Name (L)	QUITO	SI		OID 2.5.4.7
1.4.3. Organizational Unit Name (OU)	UNIDAD DE CERTIFICACION ELECTRONICA	NO		OID 2.5.4.11
1.4.4. Organization Name (O)	DICERT S.A.	SI		OID 2.5.4.10
1.4.5. Common Name (CN)	Nombre de la AC Subordinada "DICERT AC SUBORDINADA"	SI		OID 2.5.4.3
1.4.6. Organization Identifier	VATEC-1793151884001	NO		OID 2.5.4.97 codificación acorde la ETSI EN 319 412-1 RFC 5280 establece como no obligatorio
1.5. Validity	Se recomienda (máximo 5 años)	SI		
1.5.1. Not Before	Fecha de inicio de validez	SI		YYMMDDHHMMSSZ
1.5.2. Not After	Fecha de expiración	SI		YYMMDDHHMMSSZ
1.6. Subject		SI		
1.6.1. Country Name (C)	EC	SI		OID 2.5.4.6
1.6.2. Locality Name (L)	QUITO	SI		OID 2.5.4.7
1.6.3. Organizational Unit Name (OU)	UNIDAD DE CERTIFICACION ELECTRONICA	SI		OID 2.5.4.11
1.6.4. Organization Name (O)	DICERT S.A.	SI		OID 2.5.4.10
1.6.5. Common Name (CN)	DICERT AC SUBORDINADA	SI		OID 2.5.4.3
1.6.6. Organization Identifier	VATEC-1793151884001	NO		OID 2.5.4.97 codificación acorde la ETSI EN 319 412-1 RFC 5280 establece como no obligatorio
1.7. Subject Public Key Info		SI		

 Certificamos Información Digital	PERFILES DE CERTIFICADOS DICERT		
	Revisado: Galo Becerra - GG	Código: PCD-DC-GG-014	
		Versión: 2.0	
		Clasificación de Información: DOCUMENTO CONFIDENCIAL	

1.7.1. AlgorithmIdentifier				
1.7.1.1. Algorithm	RSA encryption	SI		OID 1.2.840.113549.1.1.1
1.7.1.2. Parameters	No aplicable	NO		
1.7.2. SubjectPublicKey	Clave pública codificada de acuerdo con el algoritmo criptográfico. 2048 bits	SI		
2. Extensions				
2.1. Authority Key Identifier	Identificador de la clave del Issuer	NO	NO	OID 2.5.29.35 (Marcado como NO crítico según EN 319412-2) No es obligatorio siempre y cuando la clave pública de la AC se distribuya en forma de certificado "AUTOFIRMADO"
2.1.1. KeyIdentifier		NO		Derivado de la clave pública
2.2. Subject Key Identifier	Identificador de la clave del subject	SI	NO	OID 2.5.29.14 (Marcado como NO crítico según EN 319412-2)
2.2.1. KeyIdentifier		SI		Derivado de la clave pública
2.3. Key Usage		SI	SI	OID 2.5.29.15
2.3.1. Digital Signature	Seleccionado "1"	SI		
2.3.2. Content commitment	Seleccionado "1"	SI		
2.3.3. Key Encipherment	No seleccionado. "0"			
2.3.4. Data Encipherment	No seleccionado. "0"			
2.3.5. Key Agreement	No seleccionado. "0"			
2.3.6. Key Certificate Signature	No seleccionado. "0"			
2.3.7. CRL Signature	No seleccionado. "0"			
2.3.8. Encipher Only	No seleccionado. "0"			
2.3.9. Decipher Only	No seleccionado. "0"			
2.4. Certificate Policies		SI	NO	OID 2.5.29.32 (Marcado como NO crítico según EN 319412-2)
2.4.1. Policy Information		SI		
2.4.1.1. Policy Identifier	1.3.6.1.4.1.62486.2.6.1	SI		Identificador de la política
2.4.1.2. Policy Qualifiers		SI		
2.4.1.1.1 CPS URI	https://dicert.com.ec/links/dpc	SI		OID 1.3.6.1.5.5.7.2.1 URL de la Política de Certificados de la Entidad Acreditada

 Certificamos Información Digital	PERFILES DE CERTIFICADOS DICERT		
	Revisado: Galo Becerra - GG	Código: PCD-DC-GG-014	
		Versión: 2.0	
		Clasificación de Información: DOCUMENTO CONFIDENCIAL	

2.4.1.1.2. User Notice/Explicit text	"CERTIFICADO DE VALIDACIÓN OCSP"	SI		OID 1.3.6.1.5.5.7.2.2 Texto indicativo
2.5. Subject Alternative Names		SI	NO	OID 2.5.29.17 (Marcado como NO crítico según EN 319412-2)
2.5.1. rfc822Name	soporte@dicert.com.ec	SI		
2.6. Extended Key Usage		SI	NO	OID 2.5.29.37 (Marcado como NO crítico según EN 319412-2)
2.6.1. ocspSigning	Presente (1.3.6.1.5.5.7.3.9)	SI		Transport Layer Security (TLS) World Wide Web (WWW) client authentication
2.6.2. ocspNoCheck	Presente (1.3.6.1.5.5.7.48.1.5)	SI		Para validar el certificado OCSP, para no entrar en loop (debe ser NULL)
2.7. cRLDistributionPoint		SI	NO	OID 2.5.29.31 (Marcado como NO crítico según EN 319412-2)
2.7.1 distributionPoint	https://dicert.com.ec/links/crl1	SI		http (http://) IETF RFC 7230-7235 [3] or ldap (ldap://) IETF RFC 4516 [4] scheme
2.7.2 distributionPoint	https://dicert.com.ec/links/crl2	NO		http (http://) IETF RFC 7230-7235 [3] or ldap (ldap://) IETF RFC 4516 [4] scheme
2.8 Authority Information Access		NO	NO	OID 1.3.6.1.5.5.7.1.1 (Marcado como NO crítico según EN 319412-2)
2.8.1 Access Description		NO		No es obligatorio, en este caso al ser un certificado de OCSP no pude entrar en autovalidación
2.8.1.1 Access Method	id-ad-calssuers	NO		OID 1.3.6.1.5.5.7.48.2
2.8.1.1.1 Access Location	https://dicert.com.ec/links/certac	NO		URL acceso a certificado de la AC (http://) IETF RFC 7230-7235 [3] or https (https://) IETF RFC 2818 [5]
2.10. Basic Constraints		SI	SI	OID 2.5.29.19
2.10.1. ca	FALSE	SI		

	PERFILES DE CERTIFICADOS DICERT	
	Revisado: Galo Becerra - GG	Código: PCD-DC-GG-014
		Versión: 2.0
		Clasificación de Información: DOCUMENTO CONFIDENCIAL

9. Firmas de Responsabilidad

Elaborado por:	Firma
Nombre: Paúl Quiñónez Cargo: Consultor Legal	

Aprobado por:	Firma
Nombre: Galo Becerra Cargo: Gerente General	