RESOLUCIÓN XX-ARCOTEL-2024

EL DIRECTOR EJECUTIVO DE LA AGENCIA DE REGULACIÓN Y CONTROL DE LAS TELECOMUNICACIONES

CONSIDERANDO:

Que, la Constitución de la República del Ecuador, dispone:

*"**Art. 226.-** Las instituciones del Estado, sus organismos, dependencias, las servidoras o servidores públicos y las personas que actúen en virtud de una potestad estatal ejercerán solamente las competencias y facultades que les sean atribuidas en la Constitución y la ley. Tendrán el deber de coordinar acciones para el cumplimiento de sus fines y hacer efectivo el goce y ejercicio de los derechos reconocidos en la Constitución."*.

Que, el Código Orgánico Administrativo (COA), establece:

***"Art. 94.-** Firma electrónica y certificados digitales. La actividad de la administración será emitida mediante certificados digitales de firma electrónica.*

Las personas podrán utilizar certificados de firma electrónica en sus relaciones con las administraciones públicas.".

Que, la Ley Orgánica de Telecomunicaciones (LOT), dispone:

***"Art. 144.- Competencias de la Agencia.-** Corresponde a la Agencia de Regulación y Control de las Telecomunicaciones:*

***1.** Emitir las regulaciones, normas técnicas, planes técnicos y demás actos que sean necesarios en el ejercicio de sus competencias, para que la provisión de los servicios de telecomunicaciones cumplan con lo dispuesto en la Constitución de la República y los objetivos y principios previstos en esta Ley, de conformidad con las políticas que dicte el Ministerio rector de las Telecomunicaciones y de la Sociedad de la Información. (…);*

***29.** Regular y controlar las actividades relacionadas con el comercio electrónico y firma electrónica, de conformidad con el ordenamiento jurídico vigente.".*

***"Art. 147.- Director Ejecutivo.-** La Agencia de Regulación y Control de las Telecomunicaciones será dirigida y administrada por la o el Director Ejecutivo, de libre nombramiento y remoción del Directorio.*

Con excepción de las competencias expresamente reservadas al Directorio, la o el Director Ejecutivo tiene plena competencia para expedir todos los actos necesarios para el logro de los objetivos de esta Ley y el cumplimiento de las funciones de administración, gestión, regulación y control de las telecomunicaciones y del espectro radioeléctrico, así como para regular y controlar los aspectos técnicos de la gestión de medios de comunicación social

Dirección: Av. Diego de Almagro N31-95 entre Whymper y Alpallana
Código postal: 170518 / Quito - Ecuador
Teléfono: +593-2 2947 800
www.arcotel.gob.ec

que usen frecuencias del espectro radioeléctrico o que instalen y operen redes, tales como los de audio y vídeo por suscripción.

Ejercerá sus competencias de acuerdo con lo establecido en esta Ley, su Reglamento General y las normas técnicas, planes generales y reglamentos que emita el Directorio y, en general, de acuerdo con lo establecido en el ordenamiento jurídico vigente."

"Art. 148.- Atribuciones del Director Ejecutivo.*- Corresponde a la Directora o Director Ejecutivo de la Agencia de Regulación y Control de las Telecomunicaciones: (…) 4.Aprobar la normativa para la prestación de cada uno de los servicios de telecomunicaciones, en los que se incluirán los aspectos técnicos, económicos, de acceso y legales, así como los requisitos, contenido, términos, condiciones y plazos de los títulos habilitantes y cualquier otro aspecto necesario para el cumplimiento de los objetivos de esta Ley.".*

Disposiciones Finales:

*"**Cuarta.-** La Agencia de Regulación y Control de las Telecomunicaciones ejercerá las funciones de regulación, control y administración atribuidas al Consejo Nacional de Telecomunicaciones, Superintendencia de Telecomunicaciones y Secretaría Nacional de Telecomunicaciones en la Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos, su Reglamento General y demás normativa.".*

Que, la Ley de Comercio Electrónico, Firmas y Mensajes de Datos, dispone:

*"**Art. 28.- Reconocimiento internacional de certificados de firma electrónica.-** Los certificados electrónicos emitidos por entidades de certificación extranjeras, que cumplieren con los requisitos señalados en esta ley y presenten un grado de fiabilidad equivalente, tendrán el mismo valor legal que los certificados acreditados, expedidos en el Ecuador**. El Consejo Nacional de Telecomunicaciones dictará el reglamento correspondiente para la aplicación de este artículo.***

Las firmas electrónicas creadas en el extranjero, para el reconocimiento de su validez en el Ecuador se someterán a lo previsto en esta ley y su reglamento.

Cuando las partes acuerden entre sí la utilización de determinados tipos de firmas electrónicas y certificados, se reconocerá que ese acuerdo es suficiente en derecho.

Salvo aquellos casos en los que el Estado, en virtud de convenios o tratados internacionales haya pactado la utilización de medios convencionales, los tratados o convenios que sobre esta materia se suscriban, buscarán la armonización de normas respecto de la regulación de mensajes de datos, la firma electrónica, los servicios de certificación, la contratación electrónica y telemática, la prestación de servicios electrónicos, a través de redes de información, incluido el comercio electrónico, la protección a los usuarios de

Dirección: Av. Diego de Almagro N31-95 entre Whymper y Alpallana
Código postal: 170518 / Quito - Ecuador
Teléfono: +593-2 2947 800
www.arcotel.gob.ec

estos sistemas, y el reconocimiento de los certificados de firma electrónica entre los países suscriptores.".

***"Art. 29**.- **Entidades de certificación de información.-** Son las empresas unipersonales o personas jurídicas que emiten certificados de firma electrónica y pueden prestar otros servicios relacionados con la firma electrónica, autorizadas por el Consejo Nacional de Telecomunicaciones, según lo dispuesto en esta ley y el reglamento que deberá expedir el Presidente de la República.".*

***"Art. 37.- El Organismo de regulación, autorización y registro de las entidades de certificación acreditadas.-** El Consejo Nacional de Telecomunicaciones "CONATEL", **o la entidad que haga sus veces**, será el organismo de autorización, registro y regulación de las entidades de certificación de información acreditadas. En su calidad de organismo de autorización podrá además:*

a) Cancelar o suspender la autorización a las entidades de certificación acreditadas, previo informe motivado de la Superintendencia de Telecomunicaciones;

b) Revocar o suspender los certificados de firma electrónica, cuando la entidad de certificación acreditada los emita con inobservancia de las formalidades legales, previo informe motivado de la Superintendencia de Telecomunicaciones; y

c) Las demás atribuidas en la ley y en los reglamentos."

Disposiciones Generales:

***"Primera.-** Los certificados de firmas electrónicas, emitidos por entidades de certificación de información extranjeras y acreditados en el exterior, podrán ser revalidados en el Ecuador siempre que cumplan con los términos y condiciones exigidos por la ley. La revalidación se realizará a través de una entidad de certificación de información acreditada que garantice en la misma forma que lo hace con sus propios certificados, dicho cumplimiento.".*

Que, el Reglamento General a la Ley de Comercio Electrónico, Firmas y Mensajes de Datos determina:

***"Art. 16**.- Sin perjuicio de la reglamentación que emita el CONATEL, para la aplicación del artículo 28 de la Ley No. 67, los certificados de firma electrónica emitidos en el extranjero tendrán validez legal en el Ecuador una vez obtenida la revalidación respectiva por una Entidad de Certificación de Información y Servicios Relacionados Acreditada ante el CONATEL, la cual deberá comprobar el grado de fiabilidad de dichos certificados y de quien los emite.".*

***"Art. 17**.- Régimen de acreditación de entidades de certificación de información.- Para obtener autorización de operar directamente o a través de terceros*

Dirección: Av. Diego de Almagro N31-95 entre Whymper y Alpallana
Código postal: 170518 / Quito - Ecuador
Teléfono: +593-2 2947 800
www.arcotel.gob.ec

relacionados en Ecuador, las entidades de certificación de información deberán registrarse en el CONATEL.

Los certificados de firma electrónica emitidos y revalidados por las Entidades de Certificación de Información y Servicios Relacionados Acreditadas por el CONATEL, tienen carácter probatorio.

Las entidades que habiéndose registrado y obtenido autorización para operar, directamente o a través de terceros relacionados en Ecuador, no se acrediten en el CONATEL, tendrán la calidad de entidades de certificación de información no acreditadas y están obligadas a informar de esta condición a quienes soliciten o hagan uso de sus servicios, debiendo también, a solicitud de autoridad competente, probar la suficiencia técnica y fiabilidad de los certificados que emiten.".

Que, la Ley Orgánica para la Transformación Digital y Audiovisual, determina:

"Artículo 22.- Implementación de la firma electrónica. *Los diferentes organismos de la administración pública, así como el sector privado, deberán implementar y aceptar dentro de sus diferentes procesos el uso de la firma electrónica por parte de los administrados. Será a elección del administrado la utilización de su firma manuscrita en los diferentes procesos de la administración pública o del sector privado.".*

Que, el Reglamento General a la Ley Orgánica de la Transformación Digital y Audiovisual, determina:

"Artículo 38.- De la implementación de la firma electrónica en el sector público.-*En el sector público será de uso obligatorio la firma electrónica para los procesos y servicios que brindan las entidades.*

Los servidores públicos que en el ejercicio de sus funciones suscriban documentos, deberán contar obligatoriamente, a su costo, con un certificado de firma electrónica.

Todo documento que atribuya responsabilidad de elaboración, revisión, aprobación, emisión, certificación y/o que se haya generado en el ejercicio de sus funciones, deberá ser firmado electrónicamente y conservado en su entorno digital. Las autoridades, funcionarios y servidores públicos, deberán validar los documentos firmados electrónicamente en el software oficial definido por el ente rector de la transformación digital.

El ente rector de la transformación digital emitirá las directrices para la implementación, seguimiento, evaluación y control del uso de la firma electrónica en el sector público.".

"Art. 39.- De la recepción y validación de documentos firmados electrónicamente.- *De conformidad con el artículo 22 de la Ley Orgánica para la Transformación Digital y Audiovisual, las entidades del sector público y privado*

Dirección: Av. Diego de Almagro N31-95 entre Whymper y Alpallana
Código postal: 170518 / Quito - Ecuador
Teléfono: +593-2 2947 800
www.arcotel.gob.ec

están obligados a implementar y aceptar dentro de sus diferentes procesos, documentos que hayan sido firmados electrónicamente.

Las entidades del sector público validarán los documentos que hayan sido firmados electrónicamente a través de la plataforma o mediante los mecanismos oficiales definidos por el ente rector de la transformación digital.

Las entidades del sector privado podrán validar los documentos que hayan sido firmados electrónicamente a través de cualquier software de validación, siempre y cuando este sea compatible con los certificados de firma electrónica emitidos por todas las entidades certificadoras debidamente acreditadas por la Agencia de Regulación y Control de las Telecomunicaciones.

Las autoridades que tengan a su cargo la resolución de procesos administrativos y judiciales, cualquiera que sea su naturaleza, deberán utilizar el software oficial emitido por el ente rector de la transformación digital. Los jueces, conjueces, árbitros, autoridades administrativas y cualquier otra autoridad receptarán los documentos firmados electrónicamente, y no será necesaria la presentación de documentos físicos.".

Que, la Ley Orgánica de Protección de Datos Personales, establece:

"Art. 2.-Ámbito de aplicación material.- *La presente ley se aplicará al tratamiento de datos personales contenidos en cualquier tipo de soporte, automatizados o no, así como a toda modalidad de uso posterior. La ley no será aplicable a:*

a) Personas naturales que utilicen estos datos en la realización de actividades familiares o domésticas;
b) Personas fallecidas, sin perjuicio de lo establecido en el artículo 28 de la presente Ley;
c) Datos anonimizados, en tanto no sea posible identificar a su titular. Tan pronto los datos dejen de estar disociados o de ser anónimos, su tratamiento estará sujeto al cumplimiento de las obligaciones de esta ley, especialmente la de contar con una base de licitud para continuar tratando los datos de manera no anonimizada o disociada;
d) Actividades periodísticas y otros contenidos editoriales;
e) Datos personales cuyo tratamiento se encuentre regulado en normativa especializada de igual o mayor jerarquía en materia de gestión de riesgos por desastres naturales; y, seguridad y defensa del Estado, en cualquiera de estos casos deberá darse cumplimiento a los estándares internacionales en la materia de derechos humanos y a los principios de esta ley, y como mínimo a los criterios de legalidad, proporcionalidad y necesidad;
f) Datos o bases de datos establecidos para la prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, llevado a cabo por los organismos estatales competentes en cumplimiento de sus funciones legales. En cualquiera de estos casos deberá darse cumplimiento a los estándares internacionales en la materia de derechos humanos y a los principios de esta ley, y como mínimo a los criterios de legalidad, proporcionalidad y necesidad; y

Dirección: Av. Diego de Almagro N31-95 entre Whymper y Alpallana
Código postal: 170518 / Quito - Ecuador
Teléfono: +593-2 2947 800
www.arcotel.gob.ec

g) Datos que identifican o hacen identificable a personas jurídicas. Son accesibles al público y susceptibles de tratamiento los datos personales referentes al contacto de profesionales y los datos de comerciantes, representantes y socios y accionistas de personas jurídicas y servidores públicos, siempre y cuando se refieran al ejercicio de su profesión, oficio, giro de negocio, competencias, facultades, atribuciones o cargo y se trate de nombres y apellidos, funciones o puestos desempeñados, dirección postal o electrónica, y, número de teléfono profesional. En el caso de los servidores públicos, además serán de acceso público y susceptibles de tratamiento de datos, el histórico y vigente de la declaración patrimonial y de su remuneración."

Que, el Reglamento General a la Ley Orgánica de Protección de Datos Personales, determina:

*"**Artículo 2.- Ámbito.-** Este Reglamento se aplica a todas las personas naturales y jurídicas, nacionales y extranjeras, del sector público y privado, que realicen tratamiento de datos personales, en el contexto de que sus actividades como responsable o encargado de tratamiento de datos personales, tenga lugar en el territorio ecuatoriano o no.*

El presente Reglamento también se aplica al tratamiento de datos personales por parte de personas naturales y jurídicas, que actúen como responsables y encargados del tratamiento de datos personales de titulares no residentes en Ecuador, cuando sus actividades de tratamiento sean realizadas en territorio nacional.

El presente Reglamento aplicará para los responsables y encargados del tratamiento de datos personales no establecidos en territorio ecuatoriano a quienes les resulte aplicable la legislación nacional en virtud de un contrato o de las regulaciones vigentes del derecho internacional público. Estos deberán designar a un apoderado especial de acuerdo con el artículo 3 de este Reglamento.".

Que, con Acuerdo Ministerial Nro. 181 de 15 de septiembre de 2011, el Ministerio de Telecomunicaciones y de la Sociedad de la Información, acordó determinar tipos de certificados de Persona Natural o Física, de Persona Jurídica, Representante Legal o Miembro de Empresa y de Funcionario Público; adicionalmente determinó los campos obligatorios de dichos tipos de certificados y números identificadores de campos u OID.

Que, mediante Acuerdo Ministerial Nro. 006-2015 de 27 de enero de 2015, el Ministerio de Telecomunicaciones y de la Sociedad de la Información, reforma el Acuerdo Ministerial Nro. 181 de 15 de septiembre de 2011, agregando a los literales b) de los puntos 1.2.1 y 1.2.2, del punto 1.2 lo siguiente: *"o Empleado con relación de dependencia"*

Que, con Acuerdo Ministerial Nro. 012-2016 de 23 de mayo de 2016, el Ministerio de Telecomunicaciones y de la Sociedad de la Información, resuelve reformar el Acuerdo Ministerial Nro. 181 de 15 de septiembre de 2011, eliminando la letra c)

Dirección: Av. Diego de Almagro N31-95 entre Whymper y Alpallana
Código postal: 170518 / Quito - Ecuador
Teléfono: +593-2 2947 800
www.arcotel.gob.ec

de los acápites 1.2.1 y 1.2.2 del artículo1, suprimiendo el tipo de certificado con la figura de Funcionario Público.

Que, mediante oficio Nro. MINTEL-MINTEL-2023-0181-O de 15 de marzo de 2023, el Ministerio de Telecomunicaciones y de la Sociedad de la información solicitó: ***"(…) como ente rector solicita a la Agencia de Regulación y Control de las Telecomunicaciones (ARCOTEL) generar la normativa necesaria para la regulación y control de las Entidades de Certificación acreditadas en el país acorde a los estándares internacionales y mejores prácticas.*** *Además de la consideración en agregar alguna directriz adicional basado en los estándares y mejores prácticas. (…).".*

Que, mediante oficio Nro. ARCOTEL-CREG-2023-0100-OF de 21 de agosto de 2023, el Coordinador Técnico de Regulación, solicitó a la Dirección de Asuntos Regulatorios de la Presidencia de la República, la exención de AIR, considerando que el proyecto normativo se sujeta expresamente a lo que establece la Ley de Comercio Electrónico, Firmas y Mensajes de Datos.

Que, con oficio Nro. PR-DAR-2023-0100-O de 29 de agosto de 2023, la Dirección de Asuntos Regulatorios de la Presidencia de la República señaló: *"(…) En este sentido, con base en la disposición del Artículo 28 de la Ley de Comercio Electrónico, Firmas y Mensajes de Datos, se determina que la "creación de la normativa para el reconocimiento internacional de certificados de firma electrónica"* ***queda exenta de la presentación del AIR, debido a la existencia de una disposición expresa de ley,*** *conforme a lo establecido en los lineamientos para la elaboración de los Análisis de Impacto Regulatorio, emitidos en su momento por la Subsecretaría de la Administración Pública de la Presidencia de la República, con oficio No. PR-SAP-2021-2380-O de 09 de julio de 2021.".*

Que, con memorando Nro. ARCOTEL-CREG-2024-0038-M de 15 de enero de 2024, la Coordinación Técnica de Regulación solicitó a las Coordinaciones: Técnica de Títulos Habilitantes, Técnica de Control, General Jurídica, y, Zonales, observaciones al proyecto normativo. Mediante memorandos ARCOTEL-CZO5-2024-0122-M de 22 de enero de 2024, ARCOTEL-CJUR-2024-0074-M de 23 de enero de 2024, ARCOTEL-CTHB-2024-0230-M de 24 de enero de 2024, y ARCOTEL-CCON-2024-0163-M de 23 de enero de 2024 se remiten las observaciones respectivas.

Que, con memorando Nro. ARCOTEL-CJUR-2024-0084-M de 26 de enero de 2024, la Coordinación General Jurídica remite adjunto el Informe Jurídico No. ARCOTEL-CJDA-2024-0009 de 26 de enero de 2024, en el que se concluye: *"(…)En consideración de los antecedentes, competencia y análisis expuestos, la Dirección de Asesoría Jurídica, concluye que la propuesta de "NORMA PARA EL RECONOCIMIENTO INTERNACIONAL Y REGULACIÓN DE LOS CERTIFICADOS DE FIRMA ELECTRÓNICA, PARA LAS ENTIDADES DE CERTIFICACIÓN DE INFORMACIÓN Y SERVICIOS RELACIONADOS ACREDITADAS, CON EL FIN DE GARANTIZAR LA INTEROPERABILIDAD Y ESTANDARIZACIÓN DE LOS PROCESO ELECTRÓNICOS",* ***debe ser***

Dirección: Av. Diego de Almagro N31-95 entre Whymper y Alpallana
Código postal: 170518 / Quito - Ecuador
Teléfono: +593-2 2947 800
www.arcotel.gob.ec

conocida por la Directora Ejecutiva de la ARCOTEL*, la cual en uso de sus atribuciones dispondrá de ser el caso el cumplimiento del proceso de consultas públicas respectivo, conforme lo establece la Disposición General Primera de la Ley Orgánica de Telecomunicaciones y el procedimiento determinado en el Reglamento de Consultas Públicas.".*

Que, es necesario regular a través de una Norma, el esquema de estructura de Identificadores de objeto (Object Identifier -OID) para certificados de información y servicios relacionados para las Entidades de Certificación de Información y Servicios Relacionados y la vinculación en dicha norma para los Terceros Vinculados.

Que, los OID aplicados correctamente, son la base de toda la interoperabilidad y estandarización de los procesos electrónicos de las Instituciones y Organismos señalados en el artículo 225 de la Constitución de la República del Ecuador, respecto de los certificados de información y servicios relacionados.

Que, disponer de una identificación de OID bajo la cual se construya una estructura regulada, donde los atributos de los certificados de información y servicios relacionados sean consistentes, facilitaría y potenciaría el uso de dichos certificados en el país.

Que, la Coordinación Técnica de Regulación, mediante memorando Nro. ARCOTEL-CREG-2024- 0432-M de 18 de junio de 2024, remitió a la Dirección Ejecutiva de la ARCOTEL, el informe de presentación de la "NORMA TÉCNICA PARA LA PRESTACIÓN DE LOS SERVICIOS DE INFORMACIÓN Y SERVICIOS RELACIONADOS DE LAS ENTIDADES DE CERTIFICACIÓN ACREDITADAS Y TERCEROS VINCULADOS"

Que, mediante Disposición inserta en el memorando Nro. ARCOTEL-CREG-2024-0432-M de 18 de junio de 2024, el Director Ejecutivo de la ARCOTEL, con sujeción a la Disposición General Primera de la Ley Orgánica de Telecomunicaciones, que regula el procedimiento de Consultas Públicas, en concordancia con lo dispuesto en el Reglamento de Consultas Públicas aprobado con Resolución No. 003-03-ARCOTEL-2015 de 28 de mayo de 2015, autorizó la ejecución del procedimiento de consultas públicas, para la "NORMA PARA LA PRESTACIÓN DE LOS SERVICIOS DE INFORMACIÓN Y SERVICIOS RELACIONADOS DE LAS ENTIDADES DE CERTIFICACIÓN ACREDITADAS TERCEROS VINCULADOS".

Que, el proceso de Consultas Públicas para la emisión de la "NORMA TÉCNICA PARA LA PRESTACIÓN DE LOS SERVICIOS DE INFORMACIÓN Y SERVICIOS RELACIONADOS DE LAS ENTIDADES DE CERTIFICACIÓN ACREDITADAS TERCEROS VINCULADOS", se efectuó de conformidad con la Disposición anteriormente citada, de acuerdo al siguiente detalle:

- El 27 de junio de 2024, se publicó la convocatoria a Audiencias Públicas en el sitio web institucional de la ARCOTEL.

Dirección: Av. Diego de Almagro N31-95 entre Whymper y Alpallana
Código postal: 170518 / Quito - Ecuador
Teléfono: +593-2 2947 800
www.arcotel.gob.ec

- Las Audiencias Públicas se realizaron el 15 de julio de 2024 a las 10:15 en la ciudad de Quito en el auditorio de la ex CZ2 ubicado en las calles Amazonas N40-71 y Gaspar de Villaroel.

Que, con memorando Nro. ARCOTEL-CREG-20XX-xxxx-M de xxxxx, la Coordinación Técnica de Regulación remitió al Director Ejecutivo de la ARCOTEL, una vez concluido el procedimiento de consultas públicas el informe técnico correspondiente y la " NORMA PARA LA PRESTACIÓN DE LOS SERVICIOS DE INFORMACIÓN Y SERVICIOS RELACIONADOS DE LAS ENTIDADES DE CERTIFICACIÓN ACREDITADAS TERCEROS VINCULADOS.", al que se adjunta el informe jurídico de legalidad emitido por la Coordinación General Jurídica, el que concluye: *"(…)……"*.

En ejercicio de sus atribuciones y facultades legales y reglamentarias,

RESUELVE:

Expedir la **"NORMA TÉCNICA PARA LA PRESTACIÓN DE LOS SERVICIOS DE INFORMACIÓN Y SERVICIOS RELACIONADOS DE LAS ENTIDADES DE CERTIFICACIÓN ACREDITADAS Y TERCEROS VINCULADOS"**

CAPÍTULO I
Aspectos generales

Artículo 1.- Objeto.- La presente norma tiene por objeto establecer los aspectos técnicos y procedimientos aplicables a la prestación de servicios de certificación de información, emisión de certificados de firma electrónica, registro de datos y sellado de tiempo, así como las obligaciones y responsabilidades de los prestadores de estos servicios.

Así también, definir los perfiles para los diferentes tipos de certificados que emiten las Entidades de Certificación de Información y Servicios Relacionados y sus Terceros Vinculados; la estructura de Identificador de Objeto *(Objet Identifier – OID)* para los perfiles de certificados de información que contiene los campos comunes, de tal manera que puedan ser reconocidos por las aplicaciones sin ningún tipo de restricción técnica, semántica u organizativa.

Artículo 2.- Ámbito de aplicación.- Esta norma técnica aplica a las Entidades de Certificación de Información y Servicios Relacionados Acreditadas, Terceros Vinculados; así como las personas naturales y jurídicas (públicas o privadas) que hacen uso de la firma electrónica y servicios relacionados.

Artículo 3.- Definiciones y Acrónimos.- Los términos técnicos empleados en esta norma técnica y no definidos, tendrán el significado establecido en la Ley de Comercio

Dirección: Av. Diego de Almagro N31-95 entre Whymper y Alpallana
Código postal: 170518 / Quito - Ecuador
Teléfono: +593-2 2947 800
www.arcotel.gob.ec

Electrónico, Firmas y Mensajes de Datos, el Reglamento General de aplicación, las adoptadas por la Unión Internacional de Telecomunicaciones (UIT), por los convenios y tratados internacionales ratificados por el Ecuador; y, las regulaciones respectivas emitidas por la ARCOTEL.

Cadena de confianza: Es una lista ordenada de certificados, que contienen un certificado de un usuario final y certificados intermedios (que representan la AC subordinada), para verificar que el emisor y todos los certificados intermedios son fidedignos.

Certificado de Miembro de Empresa / Empleado con Relación de Dependencia: Es un mensaje de datos que identifica a una persona natural o jurídica que será el signatario y su vinculación con el titular de la firma que puede ser una persona jurídica pública o privada, o con la persona natural con la que tiene relación de dependencia.

Certificado de Persona Natural: Es un mensaje de datos que identifica a la persona natural titular de la firma, mayor de edad y será responsable a título personal de todo lo que firme electrónicamente, dentro del ámbito de su actividad y límites de uso que correspondan.

Certificado de Sello Electrónico: Es un mensaje de datos que identifica a la persona jurídica pública o privada que es titular de la firma y su vinculación con el signatario, quien es responsable de su protección y custodia.

Certificado de Representante Legal: Es un mensaje de datos que identifica al representante legal o apoderado que será el signatario y su vinculación con la persona jurídica pública o privada que es el titular de la firma.

Claves Criptográficas: Es la criptografía asimétrica en la que se basa la Infraestructura de Clave Pública (PKI) emplean un par de claves (podrían ser dos pares de claves), lo que se cifra con una de ellas sólo se puede descifrar con la otra y viceversa. A una de esas claves se la denomina pública y está incorporada en el certificado electrónico, mientras que a la otra se la denomina privada y está bajo la custodia del titular del certificado.

Declaración de Prácticas de Certificación (DPC): Es un documento elaborado por una Entidad de Certificación de Información y Servicios Relacionados Acreditada donde se especifica las condiciones, políticas y procedimientos para la prestación de los servicios de certificación y contiene, entre otras cosas: la gestión de los datos de creación y verificación de firma y de los certificados, las condiciones aplicables a la solicitud, expedición, uso, suspensión y extinción de la vigencia de los certificados.

ETSI: Es el Instituto Europeo de Normas de Telecomunicaciones (European Telecommunications Standards Institute); es una organización de normalización independiente Europea.

FIPS: Del inglés, *Federal Information Processing Standards*, es un estándar emitido por la NIST.

Dirección: Av. Diego de Almagro N31-95 entre Whymper y Alpallana
Código postal: 170518 / Quito - Ecuador
Teléfono: +593-2 2947 800
www.arcotel.gob.ec

IANA: Del inglés, *Internet Assigned Numbers Authority*. Es la entidad que supervisa la asignación global de direcciones IP, sistemas autónomos, servidores raíz de nombres de dominio DNS y otros recursos relativos a los protocolos de Internet.

Identificadores de Objeto (OID): Del inglés, *Object Identifier*, son una representación numérica universal y única que permite la identificación de objetos por medio de una metodología que le asegura unicidad. El OID puede identificar: normas (Recomendaciones UIT-T, las Normas Internacionales ISO, etc.), países, empresas, proyectos, los algoritmos de encriptación, políticas de certificación, información del usuario, entre otras. El OID es ampliamente utilizado en Tecnologías de la Información y la Comunicación.

Infraestructura de clave pública (PKI): La PKI o *Public Key Infrastructure,* es la tecnología que le permite cifrar datos, firmar documentos y autenticarse mediante certificados tanto la identidad de los usuarios, dispositivos o servicios. La PKI abarca los "componentes" del sistema tecnológico: el software, personas, políticas y procedimientos necesarios para crear, administrar, almacenar, distribuir y revocar certificados de firma electrónica.

ISO: Del ingés, *Internacional Organization for Standardization*, es la Organización Internacional de Normalización

Listas de Certificados Revocados (CRL): Del inglés, *Certificate Revocation List,* es una lista de certificados revocados o suspendidos , los cuales por su naturaleza no son válidos y no debe confiar ningún usuario, ni sistema.

Módulo de Seguridad de Hardware (HSM): Son dispositivos de hardware, sólidos y resistentes a manipulaciones que aseguran los procesos criptográficos generando, protegiendo y administrando claves utilizadas para cifrar y descifrar datos y crear firmas y certificados digitales.

OCSP: Del inglés, (Online Certificate Status Protocol), es un método para determinar el estado de vigencia de un certificado.

RFC: Del inglés, *Request For Comments*, o Petición de Comentarios, es un documento cuyo contenido es una propuesta oficial para un nuevo protocolo de la red Internet que se explica con todo detalle para que en caso de ser aceptado pueda ser implementado sin ambigüedades. Se abrevia como RFC. Cada RFC tiene un título y un número asignado, que no puede repetirse ni eliminarse, aunque el documento se quede obsoleto.

RSA: Del inglés, *Rivest–Shamir–Adleman*, Es un tipo de encriptación asimétrica, que utiliza dos claves diferentes pero vinculadas. En la criptografía RSA, tanto la clave pública como la privada pueden cifrar un mensaje. Para descifrarlo se utiliza la clave opuesta a la que se utiliza para cifrar un mensaje.

Signatario: Es la persona que posee los datos de creación de la firma electrónica, quien, o en cuyo nombre, y con la debida autorización se consigna una firma electrónica.

Dirección: Av. Diego de Almagro N31-95 entre Whymper y Alpallana
Código postal: 170518 / Quito - Ecuador
Teléfono: +593-2 2947 800
www.arcotel.gob.ec

Titular de Firma.- Es la persona natural o jurídica (pública o privada) a favor de quien se ha emitido un certificado u otorgado un servicio relacionado por parte de una Entidad de Certificación de Información y Servicios Relacionados Acreditada o a través de Tercero Vinculado, por lo tanto será el propietario del certificado.

UIT-T: Sector de Normalización de las Telecomunicaciones de la Unión Internacional de Telecomunicaciones.

X.509: Es un estándar UIT-T para infraestructuras de claves públicas, que especifica, entre otras cosas, formatos estándar para certificados de claves públicas y un algoritmo de validación de la ruta de certificación.

CAPÍTULO II

Obligaciones y responsabilidades de las Entidades de certificación de información y servicios relacionados acreditadas

Artículo 4.- Obligaciones de las entidades de certificación de información y servicios relacionados acreditadas.- A más de los establecidos en la Ley de Comercio Electrónico, Firmas y Mensajes de Datos y su Reglamento General, tendrá las siguientes obligaciones:

1. Atender y resolver en el término máximo de quince (15) días las solicitudes y reclamos presentadas por los usuarios, comprobar la veracidad, autenticidad, exactitud y validez de la información suministrada por los solicitantes del servicio, respecto de su identidad y otros datos relevantes, previo a la provisión efectiva de los servicios requeridos.

2. Garantizar la protección y conservación segura de los datos personales de los usuarios, obtenidos en función de sus actividades, debiendo implementar todas las medidas de seguridad adecuadas y necesarias, para proteger los datos personales frente a cualquier riesgo, amenaza o vulnerabilidad.

3. Verificar el contenido de todos los datos que consten en los certificados de firma electrónica y actuar con diligencia a fin de que toda la información constante en los mismos sea exacta, cabal y esté en función de los términos y condiciones acordados en el contrato de prestación de servicios.

4. Mantener la confidencialidad de toda la información que no figure en los certificados electrónicos.

5. Mantener actualizada toda la infraestructura técnica empleada para la prestación de servicios de certificación de información y servicios relacionados con la firma electrónica, en función de la evolución de estándares tecnológicos internacionalmente reconocidos como fiables y que cumplan con las exigencias de seguridad necesarias, a fin de garantizar la prestación de los servicios a sus usuarios.

Dirección: Av. Diego de Almagro N31-95 entre Whymper y Alpallana
Código postal: 170518 / Quito - Ecuador
Teléfono: +593-2 2947 800
www.arcotel.gob.ec

6. Abstenerse de generar, exigir, tomar conocimiento o acceder bajo ninguna circunstancia a la clave privada de los usuarios titulares de certificados de firma electrónica.

7. Publicar en su página WEB en forma permanente e ininterrumpida lo siguiente: la Declaración de Prácticas de Certificación (DPC), políticas de seguridad, políticas de certificación, perfiles de los certificados, dirección de atención al público, dirección de correo electrónico de contacto, números telefónicos de contacto y el modelo de contrato de prestación de servicios de certificación de información y servicios relacionados con la firma electrónica a suscribir con los usuarios. Así como los certificados emitidos, revocados y suspendidos, a través de una consulta en línea y gratuita por número de serie del certificado, donde se visualice datos como: estado, fecha de emisión, fecha de caducidad, tiempo de vigencia, fecha de revocación, motivo de revocación, fecha de suspensión; estos último tres cuando aplique.

8. Poner a disposición de los solicitantes de un certificado de firma electrónica, toda la información relativa a su tramitación.

9. Remitir a la Agencia de Regulación y Control de las Telecomunicaciones ARCOTEL, con una periodicidad trimestral desagregado de manera mensual, dentro de los primeros quince (15) días del trimestre siguiente al del objeto del reporte, y conforme a los formularios que ésta establezca para el efecto, la siguiente información:

    a. Número de certificados emitidos, vigentes revocados y suspendidos, por tipo.
    b. Facturación total del mes.

10. Suministrar la información que requiera la ARCOTEL, así como a las entidades administrativas competentes o judiciales en relación con las firmas electrónicas y certificados emitidos; y, en general sobre cualquier Mensaje de Datos que se encuentre bajo su custodia y administración.

11. Informar a la Agencia de Regulación y Control de las Telecomunicaciones, en el término máximo de dos (2) días, la ocurrencia de cualquier evento que comprometa la disponibilidad y la seguridad en la prestación de los servicios de certificación de información y servicios relacionados con la firma electrónica.

12. Brindar a los usuarios el acceso vía web para que se solicite la revocación de su firma en línea. Las Entidades de Certificación Acreditadas utilizarán en el proceso de revocación de firmas de manera simultánea el protocolo de OCSP y las CRL´s. Adicionalmente debe mantener actualizada en su totalidad la Lista de Certificados Revocados (CRL) diariamente, indicando la vigencia y fecha de emisión; así como, incluir los puntos de distribución en certificados intermedios y de usuario final, cumpliendo con los estándares internacionales. Las Entidades de Certificación de Información Acreditadas, serán responsables de los daños y perjuicios que se causen a terceros por incumplimiento de esta obligación.

Dirección: Av. Diego de Almagro N31-95 entre Whymper y Alpallana
Código postal: 170518 / Quito - Ecuador
Teléfono: +593-2 2947 800
www.arcotel.gob.ec

13. Disponer de mecanismos de atención permanente e inmediata para consultas y solicitudes de revocación de certificados.

14. Notificar al usuario de manera inmediata sobre la extinción, revocación, suspensión de su certificado de firma electrónica, a la dirección electrónica y a la dirección física que hubiere señalado en el contrato de servicio.

15. Proporcionar a las personas naturales o jurídicas que confían en los certificados emitidos por la Entidad de Certificación de Información y Servicios Relacionados Acreditada, medios accesibles que permitan a éstos determinar mediante el certificado:

    a. La identificación de la Entidad de Certificación de información y Servicios Relacionados Acreditada que presta los servicios;
    b. Que el signatario nombrado en el certificado tenga bajo su control los datos de creación de la firma en el momento en que se expidió el certificado; y,
    c. Que los datos de creación de la firma eran válidos en la fecha en que se expidió el certificado o antes de ella.

16. Conservar durante toda la vigencia de la acreditación la información relativa a los certificados, las declaraciones de prácticas de certificación y políticas de certificación. Una vez concluida la vigencia de la acreditación, la información relativa a los certificados deberá ser tratada de acuerdo al ordenamiento jurídico vigente.

17. Proporcionar un servicio de Protocolo de Estado de Certificado en Línea (OCSP) que permita la verificación en tiempo real del estado actual de los certificados electrónicos emitidos, cuyo acceso será forma libre y gratuita.

18. Presentar anualmente a la ARCOTEL dentro de los primeros quince (15) días de cada año siguiente al del objeto del reporte, en el plazo de al menos un (1) año, un informe de auditoría externa de Seguridad Informática para acciones de control. No podrá auditar la misma entidad por más de cuatro (4) años consecutivos.

19. Publicar en su página web los drivers de el/los token(s) correspondientes a los modelos que distribuyen y sus actualizaciones para su correcto funcionamiento y compatibilidad con todos los sistemas operativos que aun tengan soporte por su fabricante, con su respectivo manual de usuario.

20. Remitir para aprobación a la ARCOTEL cuando se genere un nuevo certificado Raíz y/o Subordinado, así como por cada tipo de certificado; así mismo, la Entidad de Certificación Acreditada deberá publicar en su sitio web las cadenas de confianza para facilitar el consumo de los servicios para la validación de firmas.

21. Remitir al MINTEL las cadenas de confianza de los certificados que previamente fueron aprobados por la ARCOTEL.

Dirección: Av. Diego de Almagro N31-95 entre Whymper y Alpallana
Código postal: 170518 / Quito - Ecuador
Teléfono: +593-2 2947 800
www.arcotel.gob.ec

Artículo 5.- Responsabilidades de las entidades de certificación de información y servicios relacionados acreditadas.- Sin perjuicio de las responsabilidades contenidas en la Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos, su Reglamento General y regulaciones que emita la ARCOTEL, tendrá las siguientes responsabilidades:

1. Contar con una Declaración de Prácticas de Certificación (DPC), en la que se especifiquen las condiciones, políticas y el procedimiento para la solicitud, emisión, uso, suspensión/reactivación del servicio y revocación de los certificados de firma electrónica, así como, para la prestación de los servicios relacionados. Estas prácticas de certificación se establecerán en base a las recomendaciones de estándares y buenas prácticas internacionales vigentes o compatibles a los empleados internacionalmente.

   Esta declaración deberá identificarse y reconocerse en el ámbito internacional acogiendo la recomendación RFC 3647 o superiores de la Internet Engineering Task Force (IETF) relacionados a la materia, la cual establece los componentes principales, manteniendo el orden numérico del contenido de los componentes y subcomponentes, respetando lo señalado en esta recomendación manteniendo el estándar, para evitar discrecionalidades de omitir contenidos o elementos que podrían resultar relevantes y que deben estar presentes. Este documento debe contener las debidas firmas de elaboración, revisión y aprobación; así mismo deberá mantener un control del historial de cambios, con su fecha de actualización previa la presentación a la ARCOTEL.

La Declaración de Prácticas de Certificación (DPC) deberá contener como mínimo:

a) Datos de identificación de la Entidad de Certificación de Información y Servicios Relacionados Acreditada, así mismo de la persona de contacto. (Nombre, correo electrónico, dirección, número de teléfono, código postal, sitio web).

b) Nombre del documento, versión, revisiones, cambios, aprobación, publicación estado de la política, OID, fecha de aprobación, fecha de publicación, localización.

c) Condiciones de manejo de la información suministrada por los usuarios.

d) Límites de responsabilidad en la prestación de servicios de certificación de información y servicios relacionados con la firma electrónica.

e) Obligaciones de la Entidad de Certificación de Información y Servicios Relacionados Acreditada en la prestación de servicios de certificación de información y servicios relacionados con la firma electrónica.

f) Obligaciones de los usuarios y precauciones que deben observar en el manejo, uso y custodia de certificados y claves.

g) Políticas de uso y manejo de los certificados de firma electrónica.

Dirección: Av. Diego de Almagro N31-95 entre Whymper y Alpallana
Código postal: 170518 / Quito - Ecuador
Teléfono: +593-2 2947 800
www.arcotel.gob.ec

h) Administración de políticas y condiciones de manejo de servicios relacionados con la firma electrónica.

i) Introducción

j) Publicación y Repositorio

1) Publicación de información sobre certificación

2) Frecuencia de Publicación

- Lista de certificados emitidos se publicará de forma inmediata, posterior a su emisión.
- Lista de Certificados revocados (CRL) y suspendidos diariamente, y de forma extraordinaria, cada vez que se revoque o suspenda un certificado.
- Publicarán de forma inmediata cualquier modificación en las políticas y prácticas de certificación.

3) Control de acceso a los repositorios

k) Identificación y Autentificación.

l) Requisitos operativos del ciclo de vida del certificado

1) Deberá establecer el tiempo para procesar las solicitudes de certificado, en caso de superar el plazo máximo establecido deberá informar al usuario de las causas que motivan la demora, quedando liberado el usuario para anular la petición y debiendo la Entidad de Certificación Acreditada o su Tercero Vinculado realizar la devolución de cualquier cobro que haya percibido.

2) Usos de las Claves y el Certificado que incluyan información relativa a las extensiones 'Key Usage' y 'Extended Key Usage' para los distintos tipos y subtipos de certificados que una entidad acreditada pueda generar.

3) Renovación del Certificado, notificará a los usuarios sobre la caducidad del certificado por medios electrónicos con al menos 30 días, previo a la fecha de vencimiento en aquellos certificados de duración igual o mayor a un año.

4) Revocación del certificado deberá suponer la pérdida de validez y es irreversible, y la suspensión del certificado deberá suponer la pérdida temporal del Certificado y es reversible.

m) Instalaciones, Gestión y Controles Operativos.

n) Controles técnicos de Seguridad.

Dirección: Av. Diego de Almagro N31-95 entre Whymper y Alpallana
Código postal: 170518 / Quito - Ecuador
Teléfono: +593-2 2947 800
www.arcotel.gob.ec

o) Perfiles de Certificados, (CRL) Lista de Certificados Revocados y OCSP (Online Certificate Status Protocol).

1) Perfil del certificado de usuarios
2) Perfil de la Entidad de Certificación Acreditada (AC Raíz (ROOT) y AC Subordinada)
3) Perfil del CRL *(Lista de Certificados Revocados)*
4) Perfil de validación OCSP
5) Perfil de Sellado de Tiempo

p) Determinar Auditorías de cumplimiento y otras evaluaciones en el cual se incluya frecuencia o circunstancias de la auditoría, cualificación del auditor, relación entre el Auditor y la Entidad de Certificación de Información y Servicios Relacionados Auditada, aspectos cubiertos por la auditoría, acciones a emprender como resultado de la detección de incidencias, comunicación de resultados, las auditorías serán de "conformidad" con los requisitos de seguridad para revisión de su infraestructura de clave pública.

q) Otros asuntos comerciales y legales.

r) Garantías en el cumplimiento de las obligaciones que se deriven de sus actividades.

s) Costos y tarifas de los servicios de certificación de información y servicios relacionados con la firma electrónica.

2. Contar con una Declaración de Políticas de Seguridad, donde se especifiquen las condiciones y procedimientos relativos a la seguridad de la infraestructura de la Entidad de Certificación de Información y seguridad en la prestación de servicios de certificación de información y servicios relacionados con la firma electrónica. Esta declaración deberá contener como mínimo:

a) Procedimientos de seguridad para el manejo de posibles eventos, cuando:

i. La seguridad de la clave privada de la Entidad de Certificación de Información y Servicios Relacionados Acreditada se vea comprometida.

ii. El sistema de seguridad de la Entidad de Certificación de Información y Servicios Relacionados Acreditada ha sido vulnerado.

iii. Se presenten fallas en el sistema de la Entidad de Certificación de Información y Servicios Relacionados Acreditada que comprometan la seguridad, disponibilidad y prestación de los servicios.

b) Plan de contingencia para garantizar la continuidad y disponibilidad de los servicios de certificación de información y servicios relacionados con la firma electrónica.

Dirección: Av. Diego de Almagro N31-95 entre Whymper y Alpallana
Código postal: 170518 / Quito - Ecuador
Teléfono: +593-2 2947 800
www.arcotel.gob.ec

c) Procedimientos y mecanismos de seguridad para resguardo y conservación segura de la información relativa a la emisión de Certificados e información proporcionada por los usuarios.

3. Gestionar y suscribir convenios o acuerdos de reconocimiento mutuo con Entidades de Certificación internacionales, a fin de otorgar el respectivo reconocimiento y validez a las firmas electrónicas creadas sobre la base de los certificados emitidos por la Entidad de Certificación de Información y Servicios Relacionados Acreditada.

4. Contar con el personal idóneo que posea los conocimientos técnicos y la experiencia adecuada para manejar y gestionar, sobre la base de los procedimientos de seguridad pertinentes, la provisión de servicios de certificación de información y servicios relacionados con la firma electrónica.

5. Implementar y operar mecanismos de ejecución inmediata para revocar los certificados emitidos a los usuarios, a petición de éstos o por las causas previstas en la normativa aplicable.

6. Contar con una infraestructura segura para la creación y verificación del certificado de firma electrónica, así como de los servicios relacionados con la misma, que permita asegurar y garantizar la protección contra toda alteración.

7. Garantizar al usuario la prestación permanente, inmediata, oportuna, ágil y segura de los servicios de certificación de información y servicios relacionados con la firma electrónica, en los términos y condiciones acordadas en el contrato de prestación de servicios.

8. Emitir certificados únicos y que no se puedan duplicar, que contengan un identificador exclusivo que lo distinga de forma unívoca ante el resto. Los certificados se emitirán a personas mayores de edad, con plena capacidad jurídica.

9. Informar a los solicitantes y usuarios de los certificados electrónicos, sobre el nivel de confiabilidad de los mismos, los límites de uso y sobre las responsabilidades y obligaciones que el solicitante asume como usuario del servicio de certificación.

10. Capacitar, advertir e informar a los solicitantes y usuarios de servicios de certificación de información y servicios relacionados con la firma electrónica, respecto de las medidas de seguridad, condiciones, alcances, limitaciones y responsabilidades que deben observar en el uso de los servicios contratados.

CAPÍTULO III
Características técnicas de los Perfiles de los Certificados

Artículo 6.- Perfiles de Certificados.- Se establece la estructura de cada uno de los perfiles de certificado por tipo de contenedor:

a) Certificados en software o archivo p.12 - (PKCS #12).

Dirección: Av. Diego de Almagro N31-95 entre Whymper y Alpallana
Código postal: 170518 / Quito - Ecuador
Teléfono: +593-2 2947 800
www.arcotel.gob.ec

b) Certificados en Dispositivos Seguros de Creación de Firma (DSCF): Dispositivos Criptográficos Seguros, Certificados Remotos o en nube (HSM) y Certificados en Tarjeta Criptográfica.

Los certificados deberán contener toda la cadena de confianza, conforme la estructura de cada tipo de certificado detallado en los anexos a continuación:

1. Certificados de Persona Natural:

    a)Certificado de Personas Naturales – En archivo Anexo 1a

    b)Certificado de Personas Naturales – En DSCF Anexo 1b

2. Certificado de Miembro de Empresa o Empleado con Relación de dependencia:

    a)Certificado de Miembro de Empresa / Empleado con Relación de Dependencia – En archivo Anexo 2a

    b)Certificado de Miembro de Empresa / Empleado con Relación de Dependencia – En DSCF Anexo 2b

3. Certificado de Representante Legal:

    a) Certificado de Representante Legal – En archivo Anexo 3a

    b) Certificado de Representante Legal – En DSCF Anexo 3b

4. Certificado de Sello Electrónico:

    a. Certificado de Sello Electrónico – En archivo Anexo 4a

    b. Certificado de Sello Electrónico – En DSCF Anexo 4b

5) Certificado de Sellado de Tiempo - Anexo 5

6) Certificado de Autoridad de Certificación Raíz (ROOT) – Anexo 6

7) Certificado de Autoridad de Certificación Subordinada – Anexo 7

8) Certificado de Validación OCSP – Anexo 8

Artículo 7.- Recomendaciones y Estándares Internacionales.– Las Entidades de Certificación de Información y Servicios Relacionados Acreditadas, deberán utilizar los estándares y RFC (*Request for Comments)* enlistados en el presente artículo, o los estándares y recomendaciones que las reemplacen u otras con mejores características de acuerdo con las prácticas de certificación compatibles a las empleadas internacionalmente, apegados al artículo 10 del Reglamento General a la Ley Orgánica de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos.

Dirección: Av. Diego de Almagro N31-95 entre Whymper y Alpallana
Código postal: 170518 / Quito - Ecuador
Teléfono: +593-2 2947 800
www.arcotel.gob.ec

A continuación se enlistan las recomendaciones y estándares internacionales:

- Políticas de certificación y prácticas de certificación: RFC 3647 *"Internet X.509 Public Key Infrastructure. Certificate Policy and Certification Practices"*
- Perfil de los Certificados y de la Lista de Revocación (CRL): RFC - 5280 *"Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile"*
- Perfiles de Certificados: ETSI EN 319 412-1, ETSI EN 319 412-2, ETSI EN 319 412-3
- Estructura de la PKI: ITU–T RECOMMENDATION X.509 | ISO/IEC 9594–8
- Protocolo en línea del Estado del Certificado – OCSP *(Online Certificate Status Protocol)*: RFC 6960 – X.509
- Sellado de Tiempo: RFC 3161 *"Internet X.509 Public Key Infrastructure. Time-Stamp Protocol (TSP)".*
- Nivel de Seguridad: FIPS 140-2 *(Federal Information Processing Standards)* / COMMON CRITERIA *(ISO/IEC 15408)*
- Generación de las claves: RSA.

Artículo 8.- De los Campos OID (Identificador de Objeto).- Los campos indicados en los Anexos 1a, 1b, 2a, 2b, 3a, 3b, 4a, 4b, 5, 6, 7 y 8, deberán mantener el orden especificado; los campos opcionales y obligatorios se encuentran definidos por cada perfil, los cuales deben emitir las Entidades de Certificación de Información y Servicios Relacionados Acreditadas, según la especificidad del certificado. Así mismo, cualquier plataforma, sistema informático o aplicativo que requiera el uso de los certificados electrónicos, deberá mantener la numeración de identificadores de campos definidos, los cuales se encuentran acorde a las mejores prácticas y recomendaciones internacionales.

Cada Entidad de Certificación de Información y Servicios Relacionados Acreditada podrá incluir campos opcionales que considere necesarios al tipo de certificado, dichas modificaciones deberán ser notificadas a la ARCOTEL para el respectivo registro. Los campos incluidos no deberán en ningún caso afectar a la estructura definida en la presente norma.

CAPÍTULO IV
Seguridad de la Información de los Certificados

Artículo 9.- Mecanismos de Seguridad.- Las Entidades de Certificación de Información y Servicios Relacionados Acreditada y sus Terceros Vinculados, deberán utilizar mecanismos de seguridad, que garanticen la confidencialidad, integridad, autenticación, no repudio, control de acceso y disponibilidad de la información, contenidas en los certificados a través de herramientas criptográficas.

Dirección: Av. Diego de Almagro N31-95 entre Whymper y Alpallana
Código postal: 170518 / Quito - Ecuador
Teléfono: +593-2 2947 800
www.arcotel.gob.ec

Las claves privadas de la Entidad de Certificación Acreditada se deberán almacenar y utilizar dentro de un dispositivo criptográfico seguro que cumpla con el perfil de protección ISO apropiado. Se recomienda la utilización de FIPS 140-2 Nivel 3 y/o Common Criteria (ISO/IEC 15408) EAL4+ o superiores para seguridad de la Infraestructura de la Clave Pública (PKI), al ser estándares recomendados internacionalmente. Este nivel debe estar basado en la evaluación de riesgos y requisitos comerciales, asegurando que los módulos criptográficos están bien protegidos tanto física como lógicamente.

Estos mecanismos deberán estar basados en las recomendaciones de la Unión Internacional de Telecomunicaciones (UIT) que son concordantes con Normas y Estándares Internacionales ISO/CEI de la Organización Internacional de Normalización y la Comisión Electrotécnica Internacional, y las IETF - RFC (Internet Engineering Task Force - Request for Comments) y los estándares de la NIST (National Institute of Standards and Technology) .

Artículo 10.- Tipo de Seguridad.- Deberá estar basado en las últimas recomendaciones de la UIT-T X.509 (UIT-T X. 509 | ISO/CEI 9594-8), que definen un marco para los certificados de clave pública (Public Key Infrastructure - PKI), la infraestructura de gestión de privilegios (Privilege Management Infrastructure - PMI) define la estructura y el formato de los certificados, así como los procedimientos para su emisión y validación.

Para garantizar la seguridad de los certificados, se recomienda utilizar algoritmos de cifrado fuertes de encriptación que se encuentren disponibles acorde al avance tecnológico.

Artículo 11.- Consideraciones generales respecto de las claves criptográficas (privadas y/o públicas). - Deberán cumplirse los siguientes requerimientos mínimos:

a) El par de claves deberá ser generado únicamente por la Entidad de Certificación de Información y Servicios Relacionados Acreditada utilizando infraestructura o servicios propia o de terceros, y deberá mantener control sobre el proceso de generación de sus claves criptográficas

b) El medio de generación y almacenamiento de la clave privada utilizada en la generación de la firma deberá asegurar que:

- La clave privada sea única. Deberán utilizar como buenas prácticas aspectos como la longitud mínima, combinaciones de letras mayúsculas y minúsculas, números y caracteres especiales.

- No pueda ser deducida y se encuentre protegida contra réplicas fraudulentas, realizadas con las tecnologías disponibles a la fecha.

- Pueda ser eficazmente protegida por la Entidad de Certificación de Información y Servicios Relacionados Acreditada contra su utilización indebida.

Dirección: Av. Diego de Almagro N31-95 entre Whymper y Alpallana
Código postal: 170518 / Quito - Ecuador
Teléfono: +593-2 2947 800
www.arcotel.gob.ec

- El transporte entre el dispositivo de generación y el de almacenamiento se realice en forma segura.

- La clave privada de la Entidad de Certificación Acreditada debe almacenarse en un entorno seguro y protegido contra accesos no autorizados. Esto deberá incluir el uso de hardware de seguridad dedicado, como módulos de seguridad de hardware (HSM), que proporcionan un entorno seguro para la generación y almacenamiento de claves criptográficas.

- Para el control de acceso a la clave privada de la Entidad de Certificación Acreditada debe restringirse a un número limitado de personas autorizadas. Se deben implementar controles de acceso adecuados, como autenticación multifactor (contraseñas y tokens de seguridad), y se deben mantener registros de acceso para realizar un seguimiento de quién ha accedido a la clave y cuándo.

c) Deberá mantener procedimientos y controles que aseguren que el certificado de firma electrónica del usuario final pasará de estado “Vigente” a “Caducado” al finalizar su ciclo de vida.

d) Deberá garantizar los niveles de resguardo de las claves criptográficas y la imposibilidad de que un tercero pueda acceder a ellas y producir su activación o alteración.

e) Deberá mantener procedimientos y controles que aseguren la confidencialidad de las claves archivadas.

f) Se deberá mantener controles que aseguren que los certificados nuevos y renovados sean generados de acuerdo con sus políticas, prácticas y procedimientos.

g) Deberá mantener contratos y acuerdos de nivel de servicio que garanticen la integridad, disponibilidad y seguridad señalados en este documento con el tercero que provea la infraestructura o servicio para la generación de las claves, de ser el caso.

Artículo 12.- Almacenamiento, respaldo y recuperación de las claves criptográficas de la Entidad de Certificación de Información y Servicios Relacionados Acreditada.- La Entidad de Certificación de Información y Servicios Relacionados Acreditada a través de su infraestructura o servicios propia o de terceros, deberá mantener el control sobre las claves criptográficas durante su almacenamiento y sobre sus copias de respaldo, además deberá disponer de procedimientos para realizar la recuperación de sus claves a partir de sus copias de respaldo.

Artículo 13.- Longitud de la Clave Criptográfica (privadas y/o públicas). - Deberán respetarse las siguientes longitudes mínimas acorde con Public Key Cryptographic Standards (PKCS):

Dirección: Av. Diego de Almagro N31-95 entre Whymper y Alpallana
Código postal: 170518 / Quito - Ecuador
Teléfono: +593-2 2947 800
www.arcotel.gob.ec

a) Las claves criptográficas que utilicen Entidad de Certificación de Información y Servicios Relacionados Acreditada no podrán ser inferiores a CUATRO MIL NOVENTA Y SEIS (4096) bits con los algoritmos RSA, sin embargo se puede utilizar algoritmos con mayor robustez de acuerdo al avance tecnológico.

b) Las claves criptográficas que utilice el usuario final, no podrán ser inferiores a DOS MIL CUARENTA Y OCHO (2048) bits con los algoritmos RSA, sin embargo se puede utilizar algoritmos con mayor robustez de acuerdo al avance tecnológico.

c) Las claves criptográficas que utilicen las Entidad de Certificación de Información y Servicios Relacionados Acreditada para realizar los procesos tales como emisiones, renovaciones, revocaciones y demás servicios de certificación, deberán mantenerse permanentemente bajo su control y no podrán ser inferiores a DOS MIL CUARENTA Y OCHO (2048) bits con los algoritmos RSA, sin embargo se puede utilizar algoritmos con mayor robustez de acuerdo al avance tecnológico.

Artículo 14.- Medidas de Seguridad Tecnológicas.- Las Entidades de Certificación de Información y Servicios Relacionados Acreditadas y sus Terceros Vinculados, con la finalidad de evitar suplantaciones de identidad y/o vulneración en sus sistemas informáticos deberán contar con al menos las siguientes medidas de seguridad tecnológicas:

a) Contar como parte de su infraestructura tecnológica, con protocolos de seguridad que realicen las funciones de autenticación y validación de los usuarios; autorización y uso de los de recursos o servicios;

b) Según la política de seguridad de la Entidad de Certificación Acreditada y Servicios Relacionados y su clasificación de la información, deberá cifrar la información en reposo o en tránsito, incluso en dispositivos electrónicos y de almacenamiento, extraíbles o móviles; debiendo asegurarse de que los protocolos utilizados sean seguros y se guíen por estándares y buenas prácticas internacionales;

c) Contar con desarrollo de software seguros y adecuados, acorde al avance tecnológico y mejores prácticas internacionales;

d) El software o servicio web que se utilice para la emisión de certificados de firma electrónica deberá registrar al menos: accesos, nivel de operación, perfiles de usuarios, entre otra información disponible para valoración. Deberán generar reportes sobre dicha información y contemplar las seguridades por diseño, defensa en profundidad, seguridad por defecto, denegación predominada, fallo seguro, seguridad en implementación, privilegio mínimo, facilidad de uso y administración y funcionalidad mínima;

e) Mantener sincronizados todos los relojes de sus sistemas informáticos y los dispositivos que integran la plataforma;

Dirección: Av. Diego de Almagro N31-95 entre Whymper y Alpallana
Código postal: 170518 / Quito - Ecuador
Teléfono: +593-2 2947 800
www.arcotel.gob.ec

f) Disponer de canales de comunicación seguros mediante la utilización de técnicas de cifrado acorde con los estándares y buenas prácticas internacionales vigentes;

g) Utilizar la mejor tecnología disponible para la generación y validación de claves para los certificados de firma electrónica;

h) Implementar o actualizar las herramientas y mecanismos para monitorear redes y demás infraestructura tecnológica que permita detectar oportunamente eventos que atenten contra la seguridad de la información, actividad o comportamientos inusuales;

i) Contar con procesos ágiles para adquirir, probar e instalar parches para los componentes de la infraestructura tecnológica, de tal forma que los parches se mantengan actualizados; y evitar el uso de aplicaciones, sistemas operativos y manejadores de bases de datos sin el respaldo del fabricante o proveedor de actualizaciones de seguridad;

j) Contar con programas o software actualizados para detectar, proteger y eliminar software malicioso, así como revisar los ajustes de configuración y la vigencia de las licencias para garantizar el nivel de protección esperado;

k) Contar con herramientas para prevenir la suplantación de identidad y considerar la idoneidad de las mismas. Además, deberán contar con programas de capacitación constante para sus empleados sobre este tipo de amenazas y con herramientas de prevención de pérdida de datos para tener una visibilidad de los efectos ante dicho evento, de tal forma que se fortalezca la detección y prevención de la fuga de datos;

l) Adecuar los sistemas y demás componentes de la infraestructura tecnológica, para generar la capacidad de contar con un registro de información que permita detectar de forma activa e investigar incidencias, asegurándose de que los registros de actividades estén disponibles para su análisis cuando sea necesario;

m) Mantener un proceso continuo de técnicas que se enfoquen en la configuración segura de hardware y software (hardening), adicionalmente deberá realizar un pentesting de aplicaciones y análisis de vulnerabilidades de sus sistemas por una entidad externa especializada de manera anual y cuando se presenten vulnerabilidades, para la cual emitirá un informe técnico de los resultados obtenidos, para posterior seguimiento a las no conformidades presentadas en el informe, en el caso de existir;

n) Establecer procedimientos para monitorear, controlar y emitir alertas en línea, que informen oportunamente sobre el estado de sus sistemas; y,

o) Describir de manera general los métodos de verificación de datos y antecedentes, así como los perfiles considerados para la selección del personal que ocupa roles de confianza.

Dirección: Av. Diego de Almagro N31-95 entre Whymper y Alpallana
Código postal: 170518 / Quito - Ecuador
Teléfono: +593-2 2947 800
www.arcotel.gob.ec

Artículo 15.- Controles de seguridad informática.- Los requisitos técnicos específicos de seguridad informática para las Entidades de Certificación Acreditadas y sus Terceros Vinculados son:

Acceso local: La identificación se realizará mediante autenticación de multifactores, accediendo por IP interna y control de autorización previa de la MAC *(Media Access Control)* de la terminal.

a) Acceso remoto: Sólo será posible acceder a equipos configurados para este fin y según sensibilidad del servicio. El acceso deberá ser previamente autorizado y se deberá utilizar tecnologías que garanticen una conexión segura.

b) Controles operacionales:

- Todos los procedimientos de operación deberán estar debidamente documentados en los correspondientes manuales de operación.
- Deberán contar con herramientas de protección contra virus y códigos malignos.
- Realizarán mantenimiento continuo del equipamiento, con el fin de asegurar su disponibilidad e integridad continuadas y se generará evidencia suficiente para determinar la confiabilidad del equipamiento.
- Tendrán un procedimiento de salvado, borrado y eliminación segura de soportes de información, medios removibles y equipamiento obsoleto.

c) El intercambio de datos debe ser cifrados para asegurar la debida confidencialidad:

- Transmisión de datos entre los Servidores de Confianza de las Entidades de Certificación, sus Terceros Vinculados y los usuarios.

d) Control de accesos:

- Los operadores de registro, que realizan acciones durante el proceso del servicio de certificación, utilizarán técnicas de control de acceso y privilegio mínimo, de forma que estén relacionados con las acciones que realizan y se les puede responsabilizar de sus acciones.
- Los operadores de registro, deberán firmar una declaración de responsabilidad con la Entidad de Certificación Acreditada o con el Tercero Vinculado para el cumplimiento de sus actividades.
- La asignación de derechos se lleva a cabo siguiendo el principio de concesión mínima de privilegios.

Dirección: Av. Diego de Almagro N31-95 entre Whymper y Alpallana
Código postal: 170518 / Quito - Ecuador
Teléfono: +593-2 2947 800
www.arcotel.gob.ec

- Eliminación inmediata de los derechos de acceso de los operadores de registro que cambian de puesto de trabajo o abandonan la organización.
- Revisión periódica del nivel de acceso asignado a los operadores.
- La asignación de privilegios especiales se realiza “caso a caso” y se suprimen una vez terminada la causa que motivó su asignación.
- Mantener la calidad en las contraseñas.

Artículo 16.- Planes de mitigación. - Las Entidades deberán contar con planes de respuesta para minimizar el impacto ante un incidente de seguridad de la información. Estos planes deben ser probados para verificar la capacidad de respuesta e identificar brechas y oportunidades de mejora continua, como medidas y prácticas para la mitigación de incidentes, eventos y sus consecuencias; de acuerdo a las Políticas de Seguridad.

Artículo 17.- Atención virtual.- Para la emisión de un certificado de firma electrónica además de la atención presencial que deben brindar las Entidades de Certificación de Información y Servicios Relacionados Acreditadas o sus Terceros Vinculados, podrán prestar la atención de manera virtual lo cual implica la no presencia física de un usuario en cuanto a los procesos de recepción de información, entrega de documentación para la identificación y autenticación.

Para este efecto deberán implementar los mecanismos de seguridad reforzados necesarios, incluyendo al menos dos factores de autenticación independientes y seguros como los siguientes: validación biométrica, prueba de vida, biometría, para verificación de la identidad de los solicitantes de certificados en todo momento, u otros mecanismos adicionales para evitar la suplantación de identidad, Todos los mecanismos de seguridad implementados deberán ser comprobados con las bases de datos cedulación a cargo de la Entidad competente.

La Agencia de Regulación y Control de las Telecomunicaciones podrá requerir a las Entidades de Certificación de Información y Servicios Relacionados Acreditadas o sus Terceros Vinculados documentación e información adicionales sobre cualquier aspecto de la identificación que deberá ser entregado en un plazo de quince (15) días.

Artículo 18.- Entrega del producto y/o servicio.- Los mecanismos utilizados para la entrega de los certificados se realizará mediante archivo o en dispositivo criptográfico, estos deberán contar con la seguridad de la información respecto al cifrado y encriptación de la información (software criptográfico / software de cifrado) y/o elementos “seguros” que cuenten con la debida ciberseguridad, utilizando los medios y dispositivos adecuados seguros. La –entidad Acreditada deberá mantener el registro y constancia de la entrega efectiva del producto y/o servicio.

Las Entidades de Certificación de Información y Servicios Relacionados Acreditada o sus Terceros Vinculados no podrán solicitar información parcial o completa respecto de la clave privada del usuario, en caso de dispositivos criptográficos que tengan contraseñas por defecto, la Entidad de Certificación Acreditada o su tercero Vinculado solicitará al

Dirección: Av. Diego de Almagro N31-95 entre Whymper y Alpallana
Código postal: 170518 / Quito - Ecuador
Teléfono: +593-2 2947 800
www.arcotel.gob.ec

titular del certificado al momento de la emisión el cambio de la misma, así como también será el responsable de su administración.

CAPÍTULO V
Revalidación del certificado de firma electrónica emitida en el extranjero

Artículo 19.- Requisitos.- Para que los usuarios puedan revalidar el certificado de firma electrónica ante una Entidad de Certificación de Información y Servicios Relacionados Acreditada o su Tercero Vinculado, además de los requisitos contemplados en la Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos y, su Reglamento General, deberá contar con los siguientes requisitos mínimos:

1. Solicitud de servicio para revalidar la firma electrónica;
2. Presentar el o los documento(s) firmado(s) electrónicamente con firma(s) extranjera(s) en formato (PDF, XML, etc.) con el certificado de firma que se requiere validar, en caso de contar con dicho documento;
3. Presentar el documento de identificación del solicitante del servicio; y,

Artículo 20.- Procedimiento para el Reconocimiento de certificados de firma electrónica emitidos en el extranjero.- La Entidad de Certificación de Información y Servicios Relacionados Acreditada o su Tercero Vinculado deberá acoger el siguiente procedimiento para la revalidación del certificado de firma electrónica:

1. Consultar las listas de revocación de certificados (CRL) y OCSP, revisar la cadena de confianza (certificados raíz y subordinado de la Entidad de Certificación) o servicios de validación en línea para verificar si el certificado ha sido revocado;

2. Verificación de aspectos técnicos del certificado electrónico con firma emitido en el extranjero , y con base al numeral anterior comprobar el grado de fiabilidad de dichos certificados y de quien los emite;

3. Una vez realizadas las pruebas correspondientes, las Entidades de Certificación Acreditadas o su Tercero Vinculado emitirán un reporte de validación del documento firmado electrónicamente con firma emitida en el extranjero. El contenido del reporte de validación indicará si es VÁLIDO o INVÁLIDO el certificado , detallando de manera funcional y técnica las razones y motivos del resultado;

4. La Entidad de Certificación de Información y Servicios Relacionados Acreditada notificará a la ARCOTEL sobre la revalidación de los certificados emitidos por la entidad extranjera y publicará en su página web una referencia a la compatibilidad de estos certificados en Ecuador;

5. El plazo de vigencia de la revalidación será de acuerdo al plazo de vigencia otorgado por la Entidad de Certificación extranjera que se encuentra establecido en el certificado;

Dirección: Av. Diego de Almagro N31-95 entre Whymper y Alpallana
Código postal: 170518 / Quito - Ecuador
Teléfono: +593-2 2947 800
www.arcotel.gob.ec

La revalidación corresponde al certificado de firma electrónica, no así al contenido de los documentos.

CAPÍTULO VI
Sellado de Tiempo

Artículo 21.- Servicio de Sellado de Tiempo. – El servicio de sellado de tiempo incluye:

a) Recepción del mensaje de datos a sellar electrónicamente.

b) Los sistemas de información empleados por las Entidades de Certificación Acreditadas y su Tercero Vinculado deben garantizar como mínimo la fecha, hora y el registro de quien se autentico para consumir el servicio. Para efectos legales el servicio de sellado de tiempo se prestará tomando como referencia el huso horario del territorio continental ecuatoriano UTC ("Universal Time Coordinated").

c) El hash correspondiente al mensaje de datos del documento deberá ser sellado para garantizar su integridad y autenticidad de acuerdo a la Ley.

d) De manera opcional los servicios de encriptación o aseguramiento de confidencialidad cuando sea solicitado.

Artículo 22.- Responsabilidad de Servicios de Sellado de Tiempo.- Será responsabilidad de las Entidades de Certificación de Información Acreditadas o su Tercero Vinculado las siguientes:

a) Garantizar la integridad de los documentos sellados.

b) Garantizar mecanismos automáticos de sellado de tiempo sin posibilidad de cambios en los sistemas de verificación de tiempo y en el sistema de sellado de tiempo.

c) Proporcionar un sistema que garantice la disponibilidad permanente del servicio de sellado de tiempo.

d) Sincronizar al menos una vez al día sus equipos informáticos de Sellados de Tiempo a través de dispositivos del Sistema Global de Posicionamiento (GPS), protocolo NTP o similares, que permitan trasladar el tiempo UTC con un margen de error no superior a un (1) segundo.

En caso de requerirse cambios en el sistema de sellado de tiempo, deberá informarse a la ARCOTEL. Adicionalmente deberá proporcionarse un sistema seguro de registro de todas las actividades que genere un reporte automático y encriptado de las mismas que sea accesible para el ARCOTEL para fines de control y auditorias.

Artículo 23.- Tamaños de clave y criptografía. - Los parámetros a ser considerados son:

Dirección: Av. Diego de Almagro N31-95 entre Whymper y Alpallana
Código postal: 170518 / Quito - Ecuador
Teléfono: +593-2 2947 800
www.arcotel.gob.ec

- Algoritmo de Firma: El algoritmo RSA para firmar el resumen (hash) del contenido utilizando su clave privada, este proceso crea la firma del sellado de tiempo.

- Algoritmo de Hash: El algoritmo de hash criptográfico SHA-256 para calcular el resumen (hash) del contenido que se va a sellar en el tiempo.

- Formato de sellado de tiempo: El sellado de tiempo sigue el formato especificado en el RFC 3161. Este formato incluye información sobre la marca temporal, la firma, el algoritmo de hash utilizado y otros detalles relevantes.

- Al menos 2048 bits, para RSA, se consideran seguros por un período razonable en el futuro.

Estos parámetros técnicos mínimos son esenciales para asegurar la robustez y la confiabilidad del sellado de tiempo.

Artículo 24.- Clave Pública de la Entidad de Certificación Acreditada.- El sellado de tiempo estará vinculado a la Entidad de Certificación Acreditada a través de su clave pública, dicho certificado será utilizado para verificar la autenticidad del certificado del sellado de tiempo.

Artículo 25.- Declaraciones de Prácticas de Sellado de Tiempo.- Las Entidades de Certificación Acreditadas deben publicar sus prácticas y políticas de sellado de tiempo para informar a los usuarios sobre cómo gestionan y emiten los sellados de tiempo, incluyendo aspectos como la frecuencia de emisión y las medidas de seguridad implementadas.

Artículo 26.- Seguridades Operativas.- Las Entidades de Certificación de Información y Servicios Relacionados Acreditadas deberán tener:

a) **Protección de Claves Privadas:** La Entidad de Certificación Acreditada debe implementar medidas de seguridad robustas para proteger su clave privada utilizada en el certificado de sellado de tiempo.

b) **Registro y Auditoría:** Las Entidades de Certificación Acreditadas deben llevar registros detallados de todas las operaciones relacionadas con la emisión de sellado de tiempo, y estarán sujetas a auditorías para garantizar el cumplimiento de las políticas y estándares establecidos.

c) Las Entidades de Certificación de Información y Servicios Relacionados Acreditadas dispondrán de una Política de Seguridad, Declaración de Prácticas de sellado de tiempo, estructura del sellado de tiempo y procedimientos específicos para garantizar la seguridad a diferentes niveles basados en estándares y mejores prácticas internacionales.

Artículo 27.- Protocolo de Comunicación Sellado de tiempo *(Timestamping)*.- Para la comunicación entre el usuario que solicita el sellado de tiempo y la Entidad de

Dirección: Av. Diego de Almagro N31-95 entre Whymper y Alpallana
Código postal: 170518 / Quito - Ecuador
Teléfono: +593-2 2947 800
www.arcotel.gob.ec

Certificación Acreditada o su Tercero Vinculado se realizará a través de protocolos seguros definido en la RFC 3161 o superiores.

Artículo 28.- Dispositivo de almacenamiento.- Las Entidades de Certificación de Información y Servicios Relacionados Acreditadas o Terceros Vinculados, deberán emitir los certificados de sellado de tiempo en dispositivos criptográficos seguros HSM (Módulos de Seguridad de Hardware) diseñados para proporcionar un entorno seguro y confiable para operaciones criptográficas, protegiendo de manera segura contra accesos no autorizados, definidos en el estándar RFC 3161, asegurando la interoperabilidad y la uniformidad en la implementación del sellado de tiempo en diferentes sistemas y aplicaciones.

Los HSM deben cumplir con estándares de seguridad reconocidos, como los definidos por FIPS *(Federal Information Processing Standards)* y/o Common Criteria o superiores.

DISPOSICIONES GENERALES

Primera.- Las Entidades Certificación de Información y Servicios Relacionados Acreditadas deberán registrarse en la IANA (Internet Assigned Numbers Authority) con el fin de obtener un código privado de empresa (SMI Network Management Private Enterprise Codes) o identificador único OID; para su registro, operación y subsiguiente desarrollo del árbol de campos OID´s, que permita la inclusión de componentes y subcomponentes relacionados.

Segunda.- Las Entidades de Certificación de Información y Servicios Relacionados Acreditadas y sus Terceros Vinculados, deberán dar un tratamiento legítimo a los datos de las personas, acogiéndose a los principios enmarcados en el ordenamiento jurídico vigente.

Tercera.- La ARCOTEL realizará los controles necesarios a los prestadores de servicios de certificación de información tomando como referencia la Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos, el Reglamento General de aplicación y la presente norma técnica, con el objeto de garantizar el cumplimiento de la normativa vigente y de los términos y condiciones establecidos en las Acreditaciones otorgadas; así como supervisará e inspeccionará, en cualquier momento las instalaciones de los prestadores de dichos servicios.

Los prestadores de servicios de certificación de información, deberán prestar a la ARCOTEL todas las facilidades para realizar las inspecciones y proporcionarles toda la información requerida para los fines de control, de no hacerlo estarán sujetos a las sanciones de Ley.

DISPOSICION TRANSITORIA

Primera.- Los Modelos de Acreditación y de Renovación para las Entidades de Certificación de Información y Servicios Relacionados Acreditadas en la ARCOTEL otorgados previo a la entrada en vigencia de la presente Norma, no requieren la suscripción de un nueva Acreditación y/o Renovación, debiendo readecuarse en caso de

Dirección: Av. Diego de Almagro N31-95 entre Whymper y Alpallana
Código postal: 170518 / Quito - Ecuador
Teléfono: +593-2 2947 800
www.arcotel.gob.ec

renovación o cuando la Entidad de Certificación lo solicite expresamente a la Dirección Ejecutiva de la ARCOTEL.

Segunda. – La ARCOTEL a través de la Coordinación Técnica de Regulación deberá actualizar en el término de 90 días, en caso de ser necesario, los Modelos de Acreditación y de Renovación para las Entidades de Certificación de Información y Servicios Relacionados.

Tercera. – La ARCOTEL a través de la Coordinación Técnica de Títulos Habilitantes establecerá o modificará en el término de 90 días, en caso de ser necesario, los formatos o formularios para la presentación de los reportes que deben entregar las Entidades de Certificación Acreditadas, los cuales deberán ser publicados en la página web institucional.

Cuarta. – A partir de entrada en vigencia de la presente Resolución, las Entidades de Certificación de Información y Servicios Relacionados Acreditadas y sus Terceros Vinculados, tendrán el plazo de dieciocho (18) meses para realizar las adecuaciones e implementaciones necesarias en sus sistemas informáticos, para dar cumplimiento a lo establecido en la presente Norma Técnica. Mientras duren las adecuaciones e implementaciones en los sistemas informáticos, las Entidades de Certificación de Información y Servicios Relacionados Acreditadas podrán continuar emitiendo los certificados electrónicos.

La Dirección Ejecutiva de la ARCOTEL, podrá otorgar o ampliar los plazos que al efecto correspondan, para la plena aplicación de esta Disposición, previa petición motivada de las Entidades de Certificación de Información y Servicios Relacionados Acreditadas.

Quinta.- Los certificados que hayan sido emitidos previo a la entrada en vigor de la presente Norma Técnica, se mantendrán vigentes hasta la renovación, extinción, suspensión o revocación del certificado.

Sexta.- Conforme el artículo 19 del Reglamento General a la Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos, la Coordinación Técnica de Control en el plazo de dieciocho (18) meses establecerá los mecanismos y procedimientos para auditar técnicamente la actividad de las Entidades de Certificación de Información y Servicios Relacionados Acreditadas.

La presente resolución, entrará en vigencia una vez publicada en el Registro Oficial

Dado en Quito, D.M., el

DIRECTOR EJECUTIVO
AGENCIA DE REGULACIÓN Y CONTROL DE LAS TELECOMUNICACIONES

Dirección: Av. Diego de Almagro N31-95 entre Whymper y Alpallana
Código postal: 170518 / Quito - Ecuador
Teléfono: +593-2 2947 800
www.arcotel.gob.ec

Elaborado Por:	Revisado Por:	Aprobado por:
Analista Técnico de Regulación de Servicios y Redes de Telecomunicaciones	**Especialista Jefe 1**	**Coordinadora Técnica de Regulación**
Analista Jurídico de Regulación de Servicios y Redes de Telecomunicaciones	**Director Técnico de Regulación de Servicios y Redes de Telecomunicaciones**	

Dirección: Av. Diego de Almagro N31-95 entre Whymper y Alpallana
Código postal: 170518 / Quito - Ecuador
Teléfono: +593-2 2947 800
www.arcotel.gob.ec

PERFILES DE CERTIFICADOS PARA LAS ENTIDADES DE CERTIFICACIÓN ACREDITAS EN EL ARCOTEL

	PERFILES DE CERTIFICADOS ECUADOR	OID por Entidad Acreditada	ANEXOS
	Políticas de Certificados	**1.3.6.1.4.1.oid_AC.2**	
	GLOSARIO		
	De PERSONA NATURAL	**1.3.6.1.4.1.oid_AC.2.1**	
1	Certificado de Persona Natural en archivo	1.3.6.1.4.1.oid_AC.2.1.1	Anexo 1a
2	Certificado de Persona Natural en DSCF	1.3.6.1.4.1.oid_AC.2.1.2	Anexo 1b
	De MIEMBRO DE EMPRESA O EN RELACIÓN DE DEPENDENCIA	**1.3.6.1.4.1.oid_AC.2.2**	
3	Certificado de Miembro de Empresa o Relación de Dependencia en archivo	1.3.6.1.4.1.47286.102.2.2.1	Anexo 2a
4	Certificado de Miembro de Empresa o Relación de Dependencia en DSCF	1.3.6.1.4.1.47286.102.2.2.2	Anexo 2b
	De REPRESENTANTE LEGAL	**1.3.6.1.4.1.oid_AC.2.3**	
5	Certificado de Representante Legal en archivo	1.3.6.1.4.1.oid_AC.2.3.1	Anexo 3a
6	Certificado de Representante Legal custodia DSCF	1.3.6.1.4.1.oid_AC.2.3.2	Anexo 3b
	De SELLO ELECTRÓNICO	**1.3.6.1.4.1.oid_AC.2.4**	
7	Certificado de Sello Electrónico en archivo	1.3.6.1.4.1.oid_AC.2.4.1	Anexo 4a
8	Certificado de Sello Electrónico en DSCF	1.3.6.1.4.1.oid_AC.2.4.2	Anexo 4b
	De SELLADO DE TIEMPO	**1.3.6.1.4.1.oid_AC.2.5**	
9	Certificado de sellado de tiempo	1.3.6.1.4.1.oid_AC.2.5.1	Anexo 5

GLOSARIO DE TÉRMINOS UTILIZADOS

ÍNDICE

AC	Autoridad de Certificación. Se entenderá como Entidad de Certificación y Servicios Relacionados Acreditada
AC Raíz	Es la Entidad de confianza que emite certificados a las Autoridades de Certificación Subordinadas y Firma ARL´s. Se entenderá como Entidad de Certificación y Servicios Relacionados Acreditada
AC Subordinada	Es la Entidad de Confianza encargada de emitir certificados a personas naturales, personas jurídicas, de sellado de tiempo, Sello Electrónico, Validación OCSP y firmar CRL´s. Se entenderá como Entidad de Certificación y Servicios Relacionados Acreditada
Certificado Raiz	En criptografía y seguridad informática, un certificado raíz es un certificado de clave pública sin firma o autofirmado que identifica la autoridad de certificación raíz.
CRL	Del inglés, Certificate Revocation List, o Lista de Certificados Revocados
DSCF	Dispositivo Seguro de Creación de Firma
ETSI	Es el Instituto Europeo de Normas de Telecomunicaciones (European Telecommunications Standards Institute); es una organización de normalización independiente Europea.
ISO	Del ingés, Internacional Organization for Standardization, es la Organización Internacional de Normalización
LDAP	Del inglés, Lightweight Directory Access Protocol, es un protocolo a nivel de aplicación que permite el acceso a un servicio de directorio ordenado y distribuido para buscar diversa información en un entorno de red.
OID	Del inglés, Object identifier, o identificador de objeto
OID_AC	Identidicador de Objeto de la Autoridad de Certificación (Entidad de Certificación de Información y Servicios Relacionados Acreditada), Registrado en la IANA
OCSP	Del inglés, Online Certificate Status Protocol, es un método para determinar el estado de revocación
RFC	Del inglés, Request For Comments, o Petición De Comentarios
RSA	En criptografía, RSA es un sistema criptográfico de clave pública
SHA	Del inglés, Secure Hash Algorithm, son una familia de funciones de hash criptográficas publicadas por el Instituto Nacional de Estándares y Tecnología (NIST) como un estándar federal de procesamiento de información (FIPS) de EE. UU
X.509	En criptografía, X.509 es un estándar UIT-T para infraestructuras de claves públicas. X.509 especifica

REPÚBLICA DEL ECUADOR

Agencia de Regulación y Control de las Telecomunicaciones

PERSONA NATURAL EN ARCHIVO - ANEXO 1a

Campo *De Persona Natural*	en Archivo Autenticación y Firma	Oblig.	Crít.	Observaciones OID 1.3.6.1.4.1.oid_AC.2.1.1
1. Basic estructure				
1.1. Version	"2"	Sí		El literal "2" corresponde a la versión 3. X.509 v3
1.2. Serial Number	Establecido automáticamente por la AC Número identificativo único del certificado.	Sí		No puede ser un número negativo ni 0.
1.3. Signature Algorithm		Sí		
1.3.1. Algorithm	SHA-256 with RSA Signature	Sí		1.2.840.113549.1.1.11
1.3.2. Parameters	No aplicable	No		
1.4. Issuer		Sí		
1.4.1. Country Name (C)	Código del País "EC" (ISO 3166)	Sí		OID 2.5.4.6
1.4.2. Organization Name(O)	Nombre de la AC Subordinada "Organización"	Sí		OID 2.5.4.10
1.4.3. Locality Name (L)	Localidad de la AC Subordinada (Ciudad) Ej. QUITO	Sí		OID 2.5.4.7
1.4.4. Organization Identifier	Identificador de la AC Subordinada "VAT(CÓDIGO_PAÍS)-IDENTIFICADOR_ORGANIZACIÓN" Ej. VATEC-1716151413001	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	Sí		OID 2.5.4.3
1.4.6. Organizational Unit Name (OU)	Nombre de la Unidad Organizativa de la AC Subordinada Ej. UNIDAD DE FIRMA ELECTRONICA	No		OID 2.5.4.11
1.5. Validity		Sí		
1.5.1. Not Before	Fecha de inicio de validez	Sí		YYMMDDHHMMSSZ
1.5.2. Not After	Fecha de expiración	Sí		YYMMDDHHMMSSZ
1.6. Subject		Sí		
1.6.1. Country Name (C)	País donde reside el Titular de la Firma "EC" (ISO 3166)	Sí		OID 2.5.4.6
1.6.2. Locality Name (L)	Localidad del Titular de la Firma (Ciudad) ej. QUITO	Sí		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)	Sí		OID 2.5.4.4
1.6.5. Given Name	Nombres del Titular de la firma (como consta en el documento oficial)	Sí		OID 2.5.4.42
1.6.6. Serial Number	Número de cédula (IDC"Pais"-1716151413) o pasaporte (PAS"País"-A6362611) Ej. IDCEC-1716151413 o PASEC-A6362611	Sí		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	Sí		OID 2.5.4.3
1.7. Subject Public Key Info		Sí		
1.7.1. AlgorithmIdentifier				
1.7.1.1. Algorithm	RSA encryption	Sí		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	Sí		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	Sí	No	OID 2.5.29.14 (Marcado como NO crítico según EN 319412-2)
2.2.1. KeyIdentifier		Sí		Derivado de la clave pública
2.3. Key Usage		Sí	Sí	OID 2.5.29.15
2.3.1. Digital Signature	Seleccionado "1"	Sí		
2.3.2. Content commintment	Seleccionado "1"	Sí		
2.3.3. Key Encipherment	Seleccionado "1"	Sí		
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		Sí		

2.4.1.1. Policy Identifier	"1.3.6.1.4.1.oid_AC.2.1.1"	Sí		Identificador de la política de la AC
2.4.1.2. Policy Qualifiers		Sí		
2.4.1.1.1 CPS URI	"(https://www.repo_example.com/dpc/)"	Sí		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"	Sí		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"	Sí		
2.6. Extended Key Usage		Sí	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)	Sí		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)	No		Sólo se activa si 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	"(http://crl1.example.com/example1subordinada.crl)"	Sí		http (http://) IETF RFC 7230-7235 [3] or ldap (ldap://) IETF RFC 4516 [4] scheme
2.7.2. distributionPoint	"(http://crl2.example.com/example2subordinada.crl)"	No		http (http://) IETF RFC 7230-7235 [3] or ldap (ldap://) IETF RFC 4516 [4] scheme
2.8. Authority Information Access		Sí	No	OID 1.3.6.1.5.5.7.1.1 (Marcado como NO crítico según EN 319412-2)
2.8.1. Access Description		Sí		
2.8.1.1. Access Method	id-ad-ocsp	Sí		OID 1.3.6.1.5.5.7.48.1
2.8.1.1.1 Access Location	"(http://ocsp1.example.com/ocsp/)"	Sí		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	"(http://ocsp2.example.com/ocsp/)"	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	"(http://www.example.com/subordinate1.crt)"	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		Sí	Sí	OID 2.5.29.19
2.9.1. cA	FALSE	Sí		

REPÚBLICA DEL ECUADOR

Agencia de Regulación y Control de las Telecomunicaciones

PERSONA NATURAL EN DSCF - ANEXO 1b

Campo *De Persona Natural*	en Dispositivo Seguro de Creación de Firma "DSCF" Autenticación y Firma	Oblig.	Crít.	Observaciones OID 1.3.6.1.4.1.oid_AC.2.1.2
1. Basic estructure				
1.1. Version	"2"	Sí		El literal "2" corresponde a la versión 3. X.509 v3
1.2. Serial Number	Establecido automáticamente por la AC. Número identificativo único del certificado.	Sí		No puede ser un número negativo ni 0.
1.3. Signature Algorithm		Sí		
1.3.1. Algorithm	SHA-256 with RSA Signature	Sí		1.2.840.113549.1.1.11
1.3.2. Parameters	No aplicable	No		
1.4. Issuer		Sí		
1.4.1. Country Name (C)	Código del País "EC" (ISO 3166)	Sí		OID 2.5.4.6
1.4.2. Organization Name (O)	Nombre de la AC Subordinada "Organización"	Sí		OID 2.5.4.10
1.4.3. Locality Name (L)	Localidad de la AC Subordinada (Ciudad) Ej. QUITO	Sí		OID 2.5.4.7
1.4.4. Organization Identifier	Identificador de la AC Subordinada "VAT(CÓDIGO_PAÍS)-IDENTIFICADOR_ORGANIZACIÓN" Ej. VATEC-1716151413001	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	Sí		OID 2.5.4.3
1.4.6. Organizational Unit Name (OU)	Nombre de la Unidad Organizativa de la AC Subordinada Ej. UNIDAD DE FIRMA ELECTRONICA	No		OID 2.5.4.11
1.5. Validity		Sí		
1.5.1. Not Before	Fecha de inicio de validez	Sí		YYMMDDHHMMSSZ
1.5.2. Not After	Fecha de expiración	Sí		YYMMDDHHMMSSZ
1.6. Subject		Sí		
1.6.1. Country Name (C)	País donde reside el Titular de la Firma "EC" (ISO 3166)	Sí		OID 2.5.4.6
1.6.2. Locality Name (L)	Localidad del Titular de la Firma (Ciudad) ej. QUITO	Sí		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)	Sí		OID 2.5.4.4
1.6.5. Given Name	Nombres del Titular de la firma (como consta en el documento oficial)	Sí		OID 2.5.4.42
1.6.6. Serial Number	Número de cédula (IDC"Pais"-1716151413) o pasaporte (PAS"País"-A6362611) Ej. IDCEC-1716151413 o PASEC-A6362611	Sí		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	Sí		OID 2.5.4.3
1.7. Subject Public Key Info		Sí		
1.7.1. AlgorithmIdentifier				
1.7.1.1. Algorithm	RSA encryption	Sí		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	Sí		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	Sí	No	OID 2.5.29.14 (Marcado como NO crítico según EN 319412-2)
2.2.1. KeyIdentifier		Sí		Derivado de la clave pública
2.3. Key Usage		Sí	Sí	OID 2.5.29.15
2.3.1. Digital Signature	Seleccionado "1"	Sí		
2.3.2. Content commintment	Seleccionado "1"	Sí		
2.3.3. Key Encipherment	Seleccionado "1"	Sí		
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		Sí		
2.4.1.1. Policy Identifier	1.3.6.1.4.1.oid_AC.2.1.2	Sí		Identificador de la política de la AC
2.4.1.2. Policy Qualifiers		Sí		
2.4.1.1.1 CPS URI	"(https://www.repo_example.com/dpc/)"	Sí		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 DISPOSITIVO SEGURO DE CREACIÓN DE FIRMA - DSCF"	Sí		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"	Sí		
2.6. Extended Key Usage		Sí	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)	Sí		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)	No		Sólo se activa si se incluye el correo electrónico del Titular d ela Firma
2.7. cRLDistributionPoint		No	No	OID 2.5.29.31 (Marcado como NO crítico según EN 319412-2)
2.7.1. distributionPoint	"(http://crl1.example.com/example1subordinada.crl)"	Sí		http (http://) IETF RFC 7230-7235 [3] or ldap (ldap://) IETF RFC 4516 [4] scheme
2.7.2. distributionPoint	"(http://crl2.example.com/example2subordinada.crl)"	No		http (http://) IETF RFC 7230-7235 [3] or ldap (ldap://) IETF RFC 4516 [4] scheme
2.8. Authority Information Access		Sí	No	OID 1.3.6.1.5.5.7.1.1 (Marcado como NO crítico según EN 319412-2)
2.8.1. Access Description		Sí		
2.8.1.1. Access Method	id-ad-ocsp	Sí		OID 1.3.6.1.5.5.7.48.1
2.8.1.1.1 Access Location	"(http://ocsp1.example.com/ocsp/)"	Sí		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	"(http://ocsp2.example.com/ocsp/)"	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-caIssuers	No		OID 1.3.6.1.5.5.7.48.2
2.8.2.1.1 Access Location	"(http://www.example.com/subordinate1.crt)"	No		URL acceso a certificado de la CA (http://) IETF RFC 7230-7235 [3] or https (https://) IETF RFC 2818 [5]
2.9. Basic Constraints		Sí	Sí	OID 2.5.29.19
2.9.1. cA	FALSE	Sí		

REPÚBLICA DEL ECUADOR

Agencia de Regulación y Control de las Telecomunicaciones

MIEMBRO DE EMPRESA O EMPLEADO CON RELACIÓN DE DEPENDENCIA EN ARCHIVO - ANEXO 2a

Campo *De Miembro de Empresa o Relación de Dependencia*	en Archivo Autenticación y Firma	Oblig.	Crít.	Observaciones OID 1.3.6.1.4.1.oid_AC.2.2.1
1. Basic estructure				
1.1. Version	"2"	Sí		El literal "2" corresponde a la versión 3.
1.2. Serial Number	Establecido automáticamente por la AC. Número identificativo único del certificado.	Sí		No puede ser un número negativo ni 0.
1.3. Signature Algorithm		Sí		
1.3.1. Algorithm	SHA-256 with RSA Signature	Sí		1.2.840.113549.1.1.11
1.3.2. Parameters	No aplicable	No		
1.4. Issuer		Sí		
1.4.1. Country Name (C)	Código del País "EC" (ISO 3166)	Sí		OID 2.5.4.6
1.4.2. Organization Name (O)	Nombre de la AC Subordinada "Organización"	Sí		OID 2.5.4.10
1.4.3. Locality Name (L)	Localidad de la AC Subordinada (Ciudad) Ej. QUITO	Sí		OID 2.5.4.7
1.4.4. Organization Identifier	Identificador de la AC Subordinada "VAT(CÓDIGO_PAÍS)-IDENTIFICADOR_ORGANIZACIÓN" Ej. VATEC-1716151413001	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	Sí		OID 2.5.4.3
1.4.6. Organizational Unit (OU)	Nombre de la Unidad Organizativa de la AC Subordinada Ej. UNIDAD DE FIRMA ELECTRONICA	No		OID 2.5.4.11
1.5. Validity		Sí		
1.5.1. Not Before	Fecha de inicio de validez	Sí		YYMMDDHHMMSSZ
1.5.2. Not After	Fecha de expiración	Sí		YYMMDDHHMMSSZ
1.6. Subject		Sí		
1.6.1. Country Name (C)	País donde reside el Signatario "EC" (ISO 3166)	Sí		OID 2.5.4.6
1.6.2. Locality Name (L)	Localidad del Signatario (Ciudad) ej. QUITO	Sí		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	Sí		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	Sí		OID 2.5.4.12
1.6.7. Surname	Apellidos del Signatario (como consta en el documento oficial)	Sí		OID 2.5.4.4
1.6.8. Given Name	Nombres del Signatario (como consta en el documento oficial)	Sí		OID 2.5.4.42
1.6.9. Serial Number	Número de cédula (IDC"Pais"-1716151413) o pasaporte (PAS"País"-A6362611) del Signatario Ej. IDCEC-1716151413 o PASEC-A6362611	Sí		OID 2.5.4.5 Número de documento oficial codificado acorde a ETSI EN 319 412-1
1.6.10. Common Name	Nombres y Apellidos del Signatario	Sí		OID 2.5.4.3
1.7. Subject Public Key Info		Sí		
1.7.1. AlgorithmIdentifier				
1.7.1.1. Algorithm	RSA encryption	Sí		OID 1.2.840.113549.1.1.1
1.7.1.2. Parameters	No aplicable	No		
1.7.2. SubjectPublicKey	Clave pública del Signatario	Sí		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	Sí	No	OID 2.5.29.14 (Marcado como NO crítico según EN 319412-2)
2.2.1. KeyIdentifier		Sí		Derivado de la clave pública
2.3. Key Usage		Sí	Sí	OID 2.5.29.15
2.3.1. Digital Signature	Seleccionado "1"	Sí		
2.3.2. Content commintment	Seleccionado "1"	Sí		
2.3.3. Key Encipherment	Seleccionado "1"	Sí		
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		Sí		
2.4.1.1. Policy Identifier	1.3.6.1.4.1.oid_AC.2.2.1	Sí		Identificador de la política de la AC
2.4.1.2. Policy Qualifiers		Sí		
2.4.1.1.1 CPS URI	"(https://www.repo_example.com/dpc/)"	Sí		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”	Sí		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 Signatario "nombreapellido@example.com.ec"	Sí		
2.6. Extended Key Usage		Sí	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)	Sí		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)	No		Sólo se activa si 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	"(http://crl1.example.com/example1subordinada.crl)"	Sí		http (http://) IETF RFC 7230-7235 [3] or ldap (ldap://) IETF RFC 4516 [4] scheme
2.7.2. distributionPoint	"(http://crl2.example.com/example2subordinada.crl)"	No		http (http://) IETF RFC 7230-7235 [3] or ldap (ldap://) IETF RFC 4516 [4] scheme
2.8. Authority Information Access		Sí	No	OID 1.3.6.1.5.5.7.1.1 (Marcado como NO crítico según EN 319412-2)
2.8.1. Access Description		Sí		
2.8.1.1. Access Method	id-ad-ocsp	Sí		OID 1.3.6.1.5.5.7.48.1
2.8.1.1.1 Access Location	"(http://ocsp1.example.com/ocsp/)"	Sí		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	"(http://ocsp2.example.com/ocsp/)"	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	"(http://www.example.com/subordinate1.crt)"	No		URL acceso a certificado de la CA (http://) IETF RFC 7230-7235 [3] or https (https://) IETF RFC 2818 [5]
2.9. Basic Constraints		Sí	Sí	OID 2.5.29.19
2.9.1. cA	FALSE	Sí		

REPÚBLICA DEL ECUADOR

Agencia de Regulación y Control de las Telecomunicaciones

MIEMBRO DE EMPRESA O EMPLEADO CON RELACIÓN DE DEPENDENCIA EN DSCF - ANEXO 2b

Campo	en Dispositivo Seguro de Creación de Firma DSCF	Oblig.	Crít.	Observaciones OID 1.3.6.1.4.1.oid_AC.2.2.2
De Miembro de Empresa o Relación de Dependencia	Autenticación y Firma			
1. Basic estructure				
1.1. Version	"2"	Sí		El literal "2" corresponde a la versión 3.
1.2. Serial Number	Establecido automáticamente por la CA. Número identificativo único del certificado.	Sí		No puede ser un número negativo ni 0.
1.3. Signature Algorithm		Sí		
1.3.1. Algorithm	SHA-256 with RSA Signature	Sí		1.2.840.113549.1.1.11
1.3.2. Parameters	No aplicable	No		
1.4. Issuer		Sí		
1.4.1. Country Name (C)	Código del País "EC" (ISO 3166)	Sí		OID 2.5.4.6
1.4.2. Organization Name (O)	Nombre de la AC Subordinada "Organización"	Sí		OID 2.5.4.10
1.4.3. Locality Name (L)	Localidad de la AC Subordinada (Ciudad) Ej. QUITO	Sí		OID 2.5.4.7
1.4.4. Organization Identifier	Identificador de la AC Subordinada "VAT(CÓDIGO_PAÍS)-IDENTIFICADOR_ORGANIZACIÓN" Ej. VATEC-1716151413001	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	Sí		OID 2.5.4.3
1.4.6. Organizational Unit (OU)	Nombre de la Unidad Organizativa de la AC Subordinada Ej. UNIDAD DE FIRMA ELECTRONICA	No		OID 2.5.4.11
1.5. Validity		Sí		
1.5.1. Not Before	Fecha de inicio de validez	Sí		YYMMDDHHMMSSZ
1.5.2. Not After	Fecha de expiración	Sí		YYMMDDHHMMSSZ
1.6. Subject		Sí		
1.6.1. Country Name (C)	País donde reside el Signatario "EC" (ISO 3166)	Sí		OID 2.5.4.6
1.6.2. Locality Name (L)	Localidad del Signatario (Ciudad) ej. QUITO	Sí		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	Sí		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	Sí		OID 2.5.4.12
1.6.7. Surname	Apellidos del Signatario (como consta en el documento oficial)	Sí		OID 2.5.4.4
1.6.8. Given Name	Nombres del Signatario (como consta en el documento oficial)	Sí		OID 2.5.4.42
1.6.9. Serial Number	Número de cédula (IDC"Pais"-1716151413) o pasaporte (PAS"País"-A6362611) del Signatario Ej. IDCEC-1716151413 o PASEC-A6362611	Sí		OID 2.5.4.5 Número de documento oficial codificado acorde a ETSI EN 319 412-1
1.6.10. Common Name	Nombres y Apellidos del Signatario	Sí		OID 2.5.4.3
1.7. Subject Public Key Info		Sí		
1.7.1. AlgorithmIdentifier				
1.7.1.1. Algorithm	RSA encryption	Sí		OID 1.2.840.113549.1.1.1
1.7.1.2. Parameters	No aplicable	No		
1.7.2. SubjectPublicKey	Clave pública del Signatario	Sí		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	Sí	No	OID 2.5.29.14 (Marcado como NO crítico según EN 319412-2)
2.2.1. KeyIdentifier		Sí		Derivado de la clave pública
2.3. Key Usage		Sí	Sí	OID 2.5.29.15
2.3.1. Digital Signature	Seleccionado "1"	Sí		
2.3.2. Content commintment	Seleccionado "1"	Sí		
2.3.3. Key Encipherment	Seleccionado "1"	Sí		
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		Sí		
2.4.1.1. Policy Identifier	1.3.6.1.4.1.oid_AC.2.2.2	Sí		Identificador de la política de la AC
2.4.1.2. Policy Qualifiers		Sí		
2.4.1.1.1 CPS URI	"(https://www.repo_example.com/dpc/)"	Sí		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 DISPOSITIVO SEGURO DE CREACIÓN DE FIRMA - DSCF“	Sí		OID 1.3.6.1.5.5.7.2.2 Texto indicativo
2.5. Subject Alternative Names		**Sí**		
2.5.1. rfc822Name	Correo electrónico del Signatario "nombreapellido@example.com.ec"	Sí		
2.6. Extended Key Usage		Sí	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)	Sí		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)	No		Sólo se activa si 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	"(http://crl1.example.com/example1subordinada.crl)"	Sí		http (http://) IETF RFC 7230-7235 [3] or ldap (ldap://) IETF RFC 4516 [4] scheme
2.7.2. distributionPoint	"(http://crl2.example.com/example2subordinada.crl)"	No		http (http://) IETF RFC 7230-7235 [3] or ldap (ldap://) IETF RFC 4516 [4] scheme
2.8. Authority Information Access		Sí	No	OID 1.3.6.1.5.5.7.1.1 (Marcado como NO crítico según EN 319412-2)
2.8.1. Access Description		Sí		
2.8.1.1. Access Method	id-ad-ocsp	Sí		OID 1.3.6.1.5.5.7.48.1
2.8.1.1.1 Access Location	"(http://ocsp1.example.com/ocsp/)"	Sí		http (http://) IETF RFC 7230-7235 [3] or ldap (ldap://) IETF RFC 4516 [4] scheme
2.8.1.1.2. Access Location	"(http://ocsp2.example.com/ocsp/)"	No		http (http://) IETF RFC 7230-7235 [3] or ldap (ldap://) IETF RFC 4516 [4] scheme
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	"(http://www.example.com/subordinate1.crt)"	No		URL acceso a certificado de la CA (http://) IETF RFC 7230-7235 [3] or https (https://) IETF RFC 2818 [5]
2.9. Basic Constraints		Sí	Sí	OID 2.5.29.19
2.9.1. cA	FALSE	Sí		

REPÚBLICA DEL ECUADOR

Agencia de Regulación y Control de las Telecomunicaciones

REPRESENTANTE LEGAL EN ARCHIVO - ANEXO 3a

Campo *De Representante Legal*	en Archivo Autenticación y Firma	Oblig.	Crít.	Observaciones OID 1.3.6.1.4.1.oid_AC.2.3.1
1. Basic estructure				
1.1. Version	"2"	Sí		El literal "2" corresponde a la versión 3.
1.2. Serial Number	Establecido automáticamente por la AC. Número identificativo único del certificado.	Sí		No puede ser un número negativo ni 0.
1.3. Signature Algorithm		Sí		
1.3.1. Algorithm	SHA-256 with RSA Signature	Sí		1.2.840.113549.1.1.11
1.3.2. Parameters	No aplicable	No		
1.4. Issuer		Sí		
1.4.1. Country Name (C)	Código del País "EC" (ISO 3166)	Sí		OID 2.5.4.6
1.4.2. Organization Name (O)	Nombre de la AC Subordinada "Organización"	Sí		OID 2.5.4.10
1.4.3. Locality Name (L)	Localidad de la AC Subordinada (Ciudad) Ej. QUITO	Sí		OID 2.5.4.7
1.4.4. Organization Identifier	Identificador de la AC Subordinada "VAT(CÓDIGO_PAÍS)-IDENTIFICADOR_ORGANIZACIÓN" Ej. VATEC-1716151413001	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	Sí		OID 2.5.4.3
1.4.6. Organizational Unit (OU)	Nombre de la Unidad Organizativa de la AC Subordinada Ej. UNIDAD DE FIRMA ELECTRONICA	No		
1.5. Validity		Sí		
1.5.1. Not Before	Fecha de inicio de validez	Sí		YYMMDDHHMMSSZ
1.5.2. Not After	Fecha de expiración	Sí		YYMMDDHHMMSSZ
1.6. Subject		Sí		
1.6.1. Country Name (C)	País donde reside de la Persona Jurídica (Pública o Privada) "EC" (ISO 3166)	Sí		OID 2.5.4.6
1.6.2. Locality Name (L)	Localidad de la Persona Jurídica (Pública o Privada) (Ciudad) ej. QUITO	Sí		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	Sí		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. Ej. REPRESENTANTE LEGAL O APODERADO	Sí		OID 2.5.4.12
1.6.6. Surname	Apellidos del Signatario (como consta en el documento oficial)	Sí		OID 2.5.4.4
1.6.7. Given Name	Nombres del Signatario (como consta en el documento oficial)	Sí		OID 2.5.4.42
1.6.8. Serial Number	Número de cédula (IDC"Pais"-1716151413) o pasaporte (PAS"País"-A6362611) del Signatario Ej. IDCEC-1716151413 o PASEC-A6362611	Sí		OID 2.5.4.5 Número de documento oficial codificado acorde a ETSI EN 319 412-1
1.6.9. Common Name	Nombres y Apellidos del Signatario	Sí		OID 2.5.4.3
1.7. Subject Public Key Info		Sí		
1.7.1. AlgorithmIdentifier				
1.7.1.1. Algorithm	RSA encryption	Sí		OID 1.2.840.113549.1.1.1
1.7.1.2. Parameters	No aplicable	No		
1.7.2. SubjectPublicKey	Clave pública del Signatario	Sí		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	Sí	No	OID 2.5.29.14 (Marcado como NO crítico según EN 319412-2)
2.2.1. KeyIdentifier		Sí		Derivado de la clave pública
2.3. Key Usage		Sí	Sí	OID 2.5.29.15
2.3.1. Digital Signature	Seleccionado "1"	Sí		
2.3.2. Content commintment	Seleccionado "1"	Sí		
2.3.3. Key Encipherment	Seleccionado "1"	Sí		
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		Sí		
2.4.1.1. Policy Identifier	1.3.6.1.4.1.oid_AC.2.3.1	Sí		OID 1.3.6.1.5.5.7.2.1 URL de la Política de Certificados de la Entidad Acreditada
2.4.1.2. Policy Qualifiers		Sí		
2.4.1.1.1 CPS URI	"(https://www.repo_example.com/dpc/)"	Sí		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"	Sí		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 Signatario "nombreapellido@example.com.ec"	Sí		
2.6. Extended Key Usage		Sí	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)	Sí		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)	No		Sólo se activa si 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	"(http://crl1.example.com/example1subordinada.crl)"	Sí		http (http://) IETF RFC 7230-7235 [3] or ldap (ldap://) IETF RFC 4516 [4] scheme
2.7.2. distributionPoint	"(http://crl2.example.com/example2subordinada.crl)"	No		http (http://) IETF RFC 7230-7235 [3] or ldap (ldap://) IETF RFC 4516 [4] scheme
2.8. Authority Information Access		Sí	No	OID 1.3.6.1.5.5.7.1.1 (Marcado como NO crítico según EN 319412-2)
2.8.1. Access Description		Sí		
2.8.1.1. Access Method	id-ad-ocsp	Sí		OID 1.3.6.1.5.5.7.48.1
2.8.1.1.1 Access Location	"(http://ocsp1.example.com/ocsp/)"	Sí		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	"(http://ocsp2.example.com/ocsp/)"	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	"(http://www.example.com/subordinate1.crt)"	No		URL acceso a certificado de la CA (http://) IETF RFC 7230-7235 [3] or https (https://) IETF RFC 2818 [5]
2.9. Basic Constraints		Sí	Sí	OID 2.5.29.19
2.9.1. cA	FALSE	Sí		

REPÚBLICA DEL ECUADOR

Agencia de Regulación y Control de las Telecomunicaciones

REPRESENTANTE LEGAL EN DSCF - ANEXO 3b				
Campo	**en Dispositivo Seguro de Creación de Firma DSCF**	**Oblig.**	**Crít.**	**Observaciones OID 1.3.6.1.4.1.oid_AC.2.3.2**
De Representante Legal	**Autenticación y Firma**			
1. Basic estructure				
1.1. Version	"2"	Sí		El literal "2" corresponde a la versión 3.
1.2. Serial Number	Establecido automáticamente por la AC. Número identificativo único del certificado.	Sí		No puede ser un número negativo ni 0.
1.3. Signature Algorithm		Sí		
1.3.1. Algorithm	SHA-256 with RSA Signature	Sí		1.2.840.113549.1.1.11
1.3.2. Parameters	No aplicable	No		
1.4. Issuer		Sí		
1.4.1. Country Name (C)	Código del País "EC" (ISO 3166)	Sí		OID 2.5.4.6
1.4.2. Organization Name (O)	Nombre de la AC Subordinada "Organización"	Sí		OID 2.5.4.10
1.4.3. Locality Name (L)	Localidad de la AC Subordinada (Ciudad) Ej. QUITO	Sí		OID 2.5.4.7
1.4.4. Organization Identifier	Identificador de la AC Subordinada "VAT(CÓDIGO_PAÍS)-IDENTIFICADOR_ORGANIZACIÓN" Ej. VATEC-1716151413001	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	Sí		OID 2.5.4.3
1.4.6. Organizational Unit (OU)	Nombre de la Unidad Organizativa de la AC Subordinada Ej. UNIDAD DE FIRMA ELECTRONICA	No		
1.5. Validity		Sí		
1.5.1. Not Before	Fecha de inicio de validez	Sí		YYMMDDHHMMSSZ
1.5.2. Not After	Fecha de expiración	Sí		YYMMDDHHMMSSZ
1.6. Subject		Sí		
1.6.1. Country Name	País donde reside de la Persona Jurídica (Pública o Privada) "EC" (ISO 3166)	Sí		OID 2.5.4.6
1.6.2. Locality Name (L)	Localidad de la Persona Jurídica (Pública o Privada) (Ciudad) ej. QUITO	Sí		OID 2.5.4.7
1.6.3. Organization Name	Persona Jurídica (Pública o Privada) de la cual es Representante Legal o Apoderado el Signatario	Sí		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. Ej. REPRESENTANTE LEGAL O APODERADO	Sí		OID 2.5.4.12
1.6.6. Surname	Apellidos del Signatario (como consta en el documento oficial)	Sí		OID 2.5.4.4
1.6.7. Given Name	Nombres del Signatario (como consta en el documento oficial)	Sí		OID 2.5.4.42
1.6.8. Serial Number	Número de cédula (IDC"Pais"-1716151413) o pasaporte (PAS"País"-A6362611) del Signatario Ej. IDCEC-1716151413 o PASEC-A6362611	Sí		OID 2.5.4.5
1.6.9. Common Name	Nombres y Apellidos del Signatario	Sí		OID 2.5.4.3
1.7. Subject Public Key Info		Sí		
1.7.1. AlgorithmIdentifier				
1.7.1.1. Algorithm	RSA encryption	Sí		OID 1.2.840.113549.1.1.1
1.7.1.2. Parameters	No aplicable	No		
1.7.2. SubjectPublicKey	Clave pública del Signatario	Sí		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	Sí	No	OID 2.5.29.14 (Marcado como NO crítico según EN 319412-2)
2.2.1. KeyIdentifier		Sí		Derivado de la clave pública
2.3. Key Usage		Sí	Sí	OID 2.5.29.15
2.3.1. Digital Signature	Seleccionado "1"	Sí		
2.3.2. Content commintment	Seleccionado "1"	Sí		
2.3.3. Key Encipherment	Seleccionado "1"	Sí		
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		Sí		
2.4.1.1. Policy Identifier	1.3.6.1.4.1.oid_AC.2.3.2	Sí		Identificador de la política de la AC
2.4.1.2. Policy Qualifiers		Sí		
2.4.1.1.1 CPS URI	"(https://www.repo_example.com/dpc/)"	Sí		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 DISPOSITIVO SEGURO DE CREACIÓN DE FIRMA - DSCF"	Sí		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 Signatario "nombreapellido@example.com.ec"	Sí		
2.6. Extended Key Usage		Sí	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)	Sí		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)	No		Sólo se activa si 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	"(http://crl1.example.com/example1subordinada.crl)"	Sí		http (http://) IETF RFC 7230-7235 [3] or ldap (ldap://) IETF RFC 4516 [4] scheme
2.7.2. distributionPoint	"(http://crl2.example.com/example1subordinada.crl)"	No		http (http://) IETF RFC 7230-7235 [3] or ldap (ldap://) IETF RFC 4516 [4] scheme
2.8. Authority Information Access		Sí	No	OID 1.3.6.1.5.5.7.1.1 (Marcado como NO crítico según EN 319412-2)
2.8.1. Access Description		Sí		
2.8.1.1. Access Method	id-ad-ocsp	Sí		OID 1.3.6.1.5.5.7.48.1
2.8.1.1.1 Access Location	"(http://ocsp1.example.com/ocsp/)"	Sí		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	"(http://ocsp2.example.com/ocsp/)"	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	"(http://www.example.com/subordinate1.crt)"	No		URL acceso a certificado de la CA (http://) IETF RFC 7230-7235 [3] or https (https://) IETF RFC 2818 [5]
2.9. Basic Constraints		Sí	Sí	OID 2.5.29.19
2.9.1. cA	FALSE	Sí		

REPÚBLICA DEL ECUADOR

Agencia de Regulación y Control de las Telecomunicaciones

SELLO ELECTRÓNICO EN ARCHIVO - ANEXO 4a

Campo	en Archivo	Oblig.	Crít.	Observaciones OID 1.3.6.1.4.1.oid_AC.2.4.1
Cert SELLO ELECTRÓNICO	Autenticación y Firma			
1. Basic estructure				
1.1. Version	"2"	Sí		El literal "2" corresponde a la versión 3.
1.2. Serial Number	Establecido automáticamente por la AC. Número identificativo único del certificado.	Sí		No puede ser un número negativo ni 0.
1.3. Signature Algorithm		Sí		
1.3.1. Algorithm	SHA-256 with RSA Signature	Sí		1.2.840.113549.1.1.11
1.3.2. Parameters	No aplicable	No		
1.4. Issuer		Sí		
1.4.1. Country Name (C)	Código del País "EC" (ISO 3166)	Sí		OID 2.5.4.6
1.4.2. Locality Name (L)	Localidad de la AC Subordinada (Ciudad) Ej. QUITO	Sí		OID 2.5.4.7
1.4.3. Organization Name (O)	Nombre de la AC Subordinada "Organización"	Sí		OID 2.5.4.10
1.4.4. Organization Identifier	Identificador de la AC Subordinada "VAT(CÓDIGO_PAÍS)-IDENTIFICADOR_ORGANIZACIÓN" Ej. VATEC-1716151413001	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	Sí		OID 2.5.4.3
1.4.6. Organizational Unit (OU)	Nombre de la Unidad Organizativa de la AC Subordinada Ej. UNIDAD DE FIRMA ELECTRONICA	No		OID 2.5.4.11
1.5. Validity		Sí		
1.5.1. Not Before	Fecha de inicio de validez	Sí		YYMMDDHHMMSSZ
1.5.2. Not After	Fecha de expiración	Sí		YYMMDDHHMMSSZ
1.6. Subject		Sí		
1.6.1. Country Name (C)	País donde se encuentra registrada la Persona Jurídica (Pública o Privada) Titular de la Firma "EC" (ISO 3166)	Sí		OID 2.5.4.6
1.6.2. Locality Name (L)	Localidad de la Persona Jurídica (Pública o Privada) Titular de la Firma (Ciudad) ej. QUITO	Sí		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"	Sí		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
1.6.5. Organization Identifier	Número de Registro Unico de Contribuyente de la Persona Jurídica (Pública o Privada) Titular de la Firma a la que está vinculado el Sello Electrónico "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"	Sí		OID 2.5.4.5
1.6.7. Common Name	Descripción del uso que se le dará al sello electrónico. Ej. RECEPCIÓN DE DOCUMENTOS EN VENTANILLA UNICA	Sí		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		Sí		
1.7.1. AlgorithmIdentifier				
1.7.1.1. Algorithm	RSA encryption	Sí		OID 1.2.840.113549.1.1.1
1.7.1.2. Parameters	No aplicable	No		
1.7.2. SubjectPublicKey	Clave pública del Signatario	Sí		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	Sí	No	OID 2.5.29.14 (Marcado como NO crítico según EN 319412-2)
2.2.1. KeyIdentifier		Sí		Derivado de la clave pública
2.3. Key Usage		Sí	Sí	OID 2.5.29.15
2.3.1. Digital Signature	Seleccionado "1"	Sí		
2.3.2. Content commintment	Seleccionado "1"	Sí		
2.3.3. Key Encipherment	Seleccionado "1"	Sí		
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		Sí		
2.4.1.1. Policy Identifier	1.3.6.1.4.1.oid_AC.102.2.4.1	Sí		Identificador de la política de AC
2.4.1.2. Policy Qualifiers		Sí		
2.4.1.1.1 CPS URI	"(https://www.repo_example.com/dpc/)"	Sí		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 ELECTRONICO EN ARCHIVO"	Sí		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		Sí	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)	Sí		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)	No		Sólo se activa si se incluye el correo electrónico de la Persona Jurídica (Pública o Privada) Titular de la Firma (sello electrónico)
2.7. cRLDistributionPoint		No	No	OID 2.5.29.31 (Marcado como NO crítico según EN 319412-2
2.7.1. distributionPoint	"(http://crl1.example.com/example1subordinada.crl)"	Sí		http (http://) IETF RFC 7230-7235 [3] or ldap (ldap://) IETF RFC 4516 [4] scheme
2.7.2. distributionPoint	"(http://crl2.example.com/example1subordinada.crl)"rl	No		http (http://) IETF RFC 7230-7235 [3] or ldap (ldap://) IETF RFC 4516 [4] scheme
2.8. Authority Information Access		Sí	No	OID 1.3.6.1.5.5.7.1.1 (Marcado como NO crítico según EN 319412-2)
2.8.1. Access Description		Sí		
2.8.1.1. Access Method	id-ad-ocsp	Sí		OID 1.3.6.1.5.5.7.48.1
2.8.1.1.1 Access Location	"(http://ocsp1.example.com/ocsp/)"	Sí		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	"(http://ocsp2.example.com/ocsp/)"	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	"(http://www.example.com/subordinate1.crt)"	No		URL acceso a certificado de la CA (http://) IETF RFC 7230-7235 [3] or https (https://) IETF RFC 2818 [5]
2.9. Basic Constraints		Sí	Sí	OID 2.5.29.19
2.9.1. cA	FALSE	Sí		

REPÚBLICA DEL ECUADOR

Agencia de Regulación y Control de las Telecomunicaciones

SELLO ELECTRÓNICO EN DSCF - ANEXO 4b				
Campo	**en Dispositivo Seguro de Creación de Firma DSCF**	**Oblig.**	**Crít.**	**Observaciones OID 1.3.6.1.4.1.oid_AC.2.4.2**
Cert SELLO ELECTRÓNICO	**Autenticación y Firma**			
1. Basic estructure				
1.1. Version	"2"	Sí		El literal "2" corresponde a la versión 3.
1.2. Serial Number	Establecido automáticamente por la AC. Número identificativo único del certificado.	Sí		No puede ser un número negativo ni 0.
1.3. Signature Algorithm		Sí		
1.3.1. Algorithm	SHA-256 with RSA Signature	Sí		1.2.840.113549.1.1.11
1.3.2. Parameters	No aplicable	No		
1.4. Issuer		Sí		
1.4.1. Country Name (C)	Código del País "EC" (ISO 3166)	Sí		OID 2.5.4.6
1.4.2. Locality Name (L)	Localidad de la AC Subordinada (Ciudad) Ej. QUITO	Si		OID 2.5.4.7
1.4.3. Organization Name (O)	Nombre de la AC Subordinada "Organización"	Sí		OID 2.5.4.10
1.4.4. Organization Identifier	Identificador de la AC Subordinada "VAT(CÓDIGO_PAÍS)-IDENTIFICADOR_ORGANIZACIÓN" Ej. VATEC-1716151413001	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	Sí		OID 2.5.4.3
1.4.6. Organizational Unit (OU)	Nombre de la Unidad Organizativa de la AC Subordinada Ej. UNIDAD DE FIRMA ELECTRONICA	No		OID 2.5.4.11
1.5. Validity		Sí		
1.5.1. Not Before	Fecha de inicio de validez	Sí		YYMMDDHHMMSSZ
1.5.2. Not After	Fecha de expiración	Sí		YYMMDDHHMMSSZ
1.6. Subject		Sí		
1.6.1. Country Name (C)	País donde se encuentra registrada la Persona Jurídica (Pública o Privada) Titular de la Firma "EC" (ISO 3166)	Sí		OID 2.5.4.6
1.6.2. Locality Name (L)	Localidad de la Persona Jurídica (Pública o Privada) Titular de la Firma (Ciudad) ej. QUITO	Sí		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"	Sí		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
1.6.5. Organization Identifier	Número de Registro Unico de Contribuyente de la Persona Jurídica (Pública o Privada) Titular de la Firma a la que está vinculado el Sello Electrónico "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"	Sí		OID 2.5.4.5
1.6.4. Common Name	Descripción del uso que se le dará al sello electrónico. Ej. RECEPCIÓN DE DOCUMENTOS EN VENTANILLA UNICA	Sí		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
1.6.8. 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		Sí		
1.7.1. AlgorithmIdentifier				
1.7.1.1. Algorithm	RSA encryption	Sí		OID 1.2.840.113549.1.1.1
1.7.1.2. Parameters	No aplicable	No		
1.7.2. SubjectPublicKey	Clave pública del Signatario	Sí		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	Sí	No	OID 2.5.29.14 (Marcado como NO crítico según EN 319412-2)
2.2.1. KeyIdentifier		Sí		Derivado de la clave pública
2.3. Key Usage		Sí	Sí	OID 2.5.29.15
2.3.1. Digital Signature	Seleccionado "1"	Sí		
2.3.2. Content commintment	Seleccionado "1"	Sí		
2.3.3. Key Encipherment	Seleccionado "1"	Sí		
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		Sí		
2.4.1.1. Policy Identifier	1.3.6.1.4.1.oid_AC.102.2.4.2	Sí		Identificador de la política de AC
2.4.1.2. Policy Qualifiers		Sí		
2.4.1.1.1 CPS URI	"(https://www.repo_example.com/dpc/)"	Sí		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 ELECTRONICO EN DISPOSITIVO SEGURO DE CREACIÓN DE FIRMA - DSCF"	Sí		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"	No		
2.6. Extended Key Usage		Sí	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)	Sí		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)	No		Sólo se activa si se incluye el correo electrónico de la Persona Jurídica (Pública o Privada) Titular de la Firma (sello electrónico)
2.7. cRLDistributionPoint		No	No	OID 2.5.29.31 (Marcado como NO crítico según EN 319412-2
2.7.1. distributionPoint	"(http://crl1.example.com/example1subordinada.crl)"	Sí		http (http://) IETF RFC 7230-7235 [3] or ldap (ldap://) IETF RFC 4516 [4] scheme
2.7.2. distributionPoint	"(http://crl2..example.com/example1subordinada.crl)"	No		http (http://) IETF RFC 7230-7235 [3] or ldap (ldap://) IETF RFC 4516 [4] scheme
2.8. Authority Information Access		Sí	No	OID 1.3.6.1.5.5.7.1.1 (Marcado como NO crítico según EN 319412-2)
2.8.1. Access Description		Sí		
2.8.1.1. Access Method	id-ad-ocsp	Sí		OID 1.3.6.1.5.5.7.48.1
2.8.1.1.1 Access Location	"(http://ocsp1.example.com/ocsp/)"	Sí		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	(http://ocsp2.example.com/ocsp/)	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	"(http://www.example.com/subordinate1.crt)"	No		URL acceso a certificado de la CA (http://) IETF RFC 7230-7235 [3] or https (https://) IETF RFC 2818 [5]
2.9. Basic Constraints		Sí	Sí	OID 2.5.29.19
2.9.1. cA	FALSE	Sí		

REPÚBLICA DEL ECUADOR

Agencia de Regulación y Control de las Telecomunicaciones

SELLADO DE TIEMPO - ANEXO 5

Campo *Cert. Sellado de Tiempo*	Autenticación y Firma	Oblig.	Crít.	Observaciones OID 1.3.6.1.4.1.oid_AC.2.5.1
1. Basic estructure				
1.1. Version	"2"	Sí		El literal "2" corresponde a la versión 3.
1.2. Serial Number	Establecido automáticamente por la AC. Número identificativo único del certificado.	Sí		No puede ser un número negativo ni 0.
1.3. Signature Algorithm		Sí		
1.3.1. Algorithm	SHA-256 with RSA Signature	Sí		1.2.840.113549.1.1.11
1.3.2. Parameters	No aplicable	No		
1.4. Issuer		Sí		
1.4.1. Country Name (C)	Código del País "EC" (ISO 3166)	Sí		OID 2.5.4.6
1.4.2. Locality Name (L)	Localidad de la AC Subordinada (Ciudad) Ej. QUITO	Sí		OID 2.5.4.7
1.4.3. Organization Name (O)	Nombre de la AC Subordinada "Organización"	Sí		OID 2.5.4.10
1.4.4. Organization Identifier	Identificador de la AC Subordinada "VAT(CÓDIGO_PAÍS)-IDENTIFICADOR_ORGANIZACIÓN" Ej. VATEC-1716151413001	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	Sí		OID 2.5.4.3
1.4.6. Organizational Unit (OU)	Nombre de la Unidad Organizativa de la AC Subordinada Ej. UNIDAD DE FIRMA ELECTRONICA	No		OID 2.5.4.11
1.5. Validity	**(Se recomienda Hasta 5 años)**	Sí		
1.5.1. Not Before	Fecha de inicio de validez	Sí		YYMMDDHHMMSSZ
1.5.2. Not After	Fecha de expiración.	Sí		YYMMDDHHMMSSZ
1.6. Subject		Sí		
1.6.1. Country Name	País donde se encuentra registrada la Persona Jurídica (Pública o Privada) Titular de la Firma "EC" (ISO 3166)	Sí		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"	Sí		OID 2.5.4.10
1.6.3. Locality Name (L)	Localidad de la Persona Jurídica (Pública o Privada) (Ciudad) Ej. QUITO	Sí		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) ej."1793081770001"	Sí		OID 2.5.4.5
1.6.6. Common Name	Nombre del Servicio "Sellado de tiempo de la Persona Jurídica (Pública o Privada)"	Sí		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	Sí		OID 2.5.4.11
1.7. Subject Public Key Info		Sí		
1.7.1. AlgorithmIdentifier				
1.7.1.1. Algorithm	RSA encryption	Sí		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	Sí		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	Sí	No	OID 2.5.29.14 (Marcado como NO crítico según EN 319412-2)
2.2.1. KeyIdentifier		Sí		Derivado de la clave pública
2.3. Key Usage		Sí	Sí	OID 2.5.29.15
2.3.1. Digital Signature	Seleccionado "1"	Sí		
2.3.2. Content commintment	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"			
2.4. Certificate Policies		Sí	No	OID 2.5.29.32 (Marcado como NO crítico según EN 319412-2)
2.4.1. Policy Information		Sí		
2.4.1.1. Policy Identifier	1.3.6.1.4.1..oid_AC.102.2.5.1	Sí		Identificador de la política de la AC
2.4.1.2. Policy Qualifiers		Sí		
2.4.1.1.1 CPS URI	"(https://www.repo_example.com/dpc/)"	Sí		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"	Sí		OID 1.3.6.1.5.5.7.2.2 Texto indicativo
2.5. Subject Alternative Names		Sí	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"	Sí		
2.6. Extended Key Usage		Sí	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)	Sí		
2.7. cRLDistributionPoint		No	No	OID 2.5.29.31 (Marcado como NO crítico según EN 319412-2
2.7.1. distributionPoint	"(http://crl1.example.com/example1subordinada.crl)"	Sí		http (http://) IETF RFC 7230-7235 [3] or ldap (ldap://) IETF RFC 4516 [4] scheme
2.7.2. distributionPoint	"(http://crl2.example.com/example1subordinada.crl)"	No		http (http://) IETF RFC 7230-7235 [3] or ldap (ldap://) IETF RFC 4516 [4] scheme
2.8. Authority Information Access		Sí	No	OID 1.3.6.1.5.5.7.1.1 (Marcado como NO crítico según EN 319412-2)
2.8.1. Access Description		Sí		
2.8.1.1. Acces Method	id-ad-ocsp	Sí		OID 1.3.6.1.5.5.7.48.1
2.8.1.1.1 Acces Location	"(http://ocsp1.example.com/ocsp/)"	Sí		URL de acceso al OCSP (http://) IETF RFC 7230-7235 [3] or https (https://) IETF RFC 2818 [5]
2.8.1.1.2. Acces Location	"(http://ocsp2.example.com/ocsp/)"	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	"(http://www.example.com/subordinate1.crt)"	No		URL acceso a certificado de la CA (http://) IETF RFC 7230-7235 [3] or https (https://) IETF RFC 2818 [5]
2.10. Basic Constraints		Sí	Sí	OID 2.5.29.19
2.10.1. cA	FALSE	Sí		

PERFILES DE CERTIFICADOS DE ENTIDADES DE CERTIFICACIÓN ACREDITADOS		Anexos
	OID	
Autoridad de Certificación Raíz		
Certificado Raíz AC ROOT		Anexo 6
Autoridad de Certificación Subordinada		
Certificado Subordinado AC SUB		Anexo 7
Certificado de Validación OCSP	**1.3.6.1.4.1.oid_AC.2.6**	
Certificado de Validación OCSP	1.3.6.1.4.1.oid_AC.2.6.1	Anexo 8

CERTIFICADO RAÍZ - AC (ROOT) - ANEXO 6

Campo	Contenido	Obligatorio	Crít.	Observaciones OID 1.3.6.1.4.1.OID_Ac.n
1. Basic estructure				
1.1 Version	"2"	Sí		El literal "2" corresponde a la versión 3.
1.2 Serial Number	Establecido automáticamente por la AC. Número identificativo único del certificado.	Sí		No puede ser un número negativo ni 0.
1.3 Signature Algorithm		Sí		
1.3.1 Identifier	1.2.840.113549.1.1.11	Sí		1.2.840.113549.1.1.11
1.3.2 Description	SHA-256 with RSA Signature	Sí		
1.4 **Issuer**		Sí		
1.4.1 Common Name (CN)	Nombre de la AC Raíz	Sí		OID 2.5.4.3
1.4.2 Country (C)	Código del País "EC" (ISO 3166)	Sí		OID 2.5.4.6
1.4.3 Organization Name (O)	Nombre de la AC Raíz "Organización"	Sí		OID 2.5.4.10
1.4.4 Locality (L)	Localidad de la AC Raíz (Ciudad) Ej. QUITO	Si		OID 2.5.4.7
1.4.5 Organizational Unit (OU)	Nombre de la Unidad Organizativa de la AC Raíz Ej. "UNIDAD DE FIRMA ELECTRONICA"	No		OID 2.5.4.11
1.4.6 Organization Identifier	Identificador "VAT(CÓDIGO_PAÍS)-IDENTIFICADOR_ORGANIZACIÓN" Ej. VATEC-1716151413001	No		OID 2.5.4.97 codificación acorde la ETSI EN 319 412-1 RFC 5280 establece como no obligatorio
1.5 Validity		Sí		
1.5.1 Not Before	Fecha de inicio de validez	Sí		YYMMDDHHMMSSZ
1.5.2 Not After	Fecha de expiración	Sí		YYMMDDHHMMSSZ
1.6 Subject	**Mismos Datos entre Issuer y Subject (AutoFirmado)**	Sí		
1.6.1 Common Name (CN)	Nombre de la AC Raíz	Sí		OID 2.5.4.3
1.6.2 Country (C)	Código del País "EC" (ISO 3166)	Sí		OID 2.5.4.6
1.6.3 Organization Name(O)	Nombre de la AC Raíz "Organización"	Sí		OID 2.5.4.10
1.6.4 Locality (L)	Localidad de la AC Raíz(Ciudad) Ej. QUITO	Sí		OID 2.5.4.7
1.6.5 Organizational Unit (OU)	Nombre de la Unidad Organizativa de la AC Raíz Ej. "UNIDAD DE FIRMA ELECTRONICA"	No		OID 2.5.4.11
1.6.6 organizationIdentifier	"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
1.7 Subject Public Key Info	**Clave pública de la AC Raíz, codificada de acuerdo con el algoritmo criptográfico.**	Sí		
1.7.1 AlgorithmIdentifier	1.2.840.113549.1.1.1			
1.7.1.1 Algorithm	RSA encryption	Sí		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	Sí		
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 Key Identifier	Identificador de la clave del issuer	No		Derivado de la clave pública
2.2 Subject Key Identifier	Presente	Sí	No	OID 2.5.29.14 (Marcado como NO crítico según EN 319412-2)
2.2.1 KeyIdentifier	Identificador de la clave del subject	Sí		
2.3 Key Usage		Sí		OID 2.5.29.15
2.3.1 Digital Signature	No seleccionado. "0"			
2.3.2 Content commintment	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"	Sí		
2.3.7 CRL Signature	Seleccionado. "1"	Sí		
2.4 Certificate Policies	Políticas de certificación / DPC	Sí	No	OID 2.5.29.32 (Marcado como NO crítico según EN 319412-2)
2.4.1 Policy Information		Sí		
2.4.1.1 Policy Identifier	2.5.29.32.0	Sí		Identificador de la política
2.4.1.2 Policy Qualifier ID	Especificación de la DPC	Sí		
2.4.1.2.1 CPS Pointer	"(https://ejemploAC.com/public/cps/)"	Sí		
2.4.1.2.2 User Notice	"(https://web.ejemplo.com/)"	Sí		
2.5 Subject Alternative Names			No	
2.5.1 rfc822Name	Correo electrónico de la Entidad Acreditada info@ejemploAC.com	Sí		
2.6 Basic Constraints		Sí	Sí	OID 2.5.29.19
2.6.1 Subject type	cA (TRUE)	Sí		
2.6.2 Path Length Constraints	0	Sí		

REPÚBLICA DEL ECUADOR

Agencia de Regulación y Control de las Telecomunicaciones

CERTIFICADO SUBORDINADO - AC SUB - ANEXO 7

Campo	Contenido	Obligatorio	Crít.	Observaciones OID 1.3.6.1.4.1.OID_Ac.n
1. Basic estructure				
1.1 Version	"2"	Sí		El literal "2" corresponde a la versión 3. X.509 v3
1.2 Serial Number	Establecido automáticamente por la AC. Número identificativo único del certificado.	Sí		No puede ser un número negativo ni 0.
1.3 Signature Algorithm		Sí		
1.3.1 Identifier	1.2.840.113549.1.1.11	Sí		1.2.840.113549.1.1.11
1.3.2 Description	SHA-256 with RSA Signature	Sí		
1.4 **Issuer**		Sí		
1.4.1 Common Name (CN)	Nombre de la AC Raíz	Sí		OID 2.5.4.3
1.4.2 Country Name (C)	Código del País "EC" (ISO 3166)	Sí		OID 2.5.4.6
1.4.3 Organization Name (O)	Nombre de la AC Raíz "Organización"	Sí		OID 2.5.4.10
1.4.4 Locality Name(L)	Localidad de la AC Raíz(Ciudad) Ej. QUITO	Si		OID 2.5.4.7
1.4.5 Organizational Unit (OU)	Nombre de la Unidad Organizativa de AC Raíz Ej. "UNIDAD DE FIRMA ELECTRONICA"	No		OID 2.5.4.11
1.4.6 organizationIdentifier	"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
1.5 Validity		Sí		
1.5.1 Not Before	Fecha de inicio de validez	Sí		YYMMDDHHMMSSZ
1.5.2 Not After	Fecha de expiración	Sí		YYMMDDHHMMSSZ
1.6 Subject		Sí		
1.6.1 Common Name (CN)	Nombre de la AC Subordinada	Sí		OID 2.5.4.3
1.6.2 Country Name(C)	País donde reside AC Subordinada ej. "EC" (ISO 3166)	Sí		OID 2.5.4.6
1.6.3 Organization Name (O)	Nombre de la AC Raíz "Organización"	Sí		OID 2.5.4.10
1.6.4 Locality Name (L)	Localidad de la AC Subordinada (Ciudad) ej. QUITO	Sí		OID 2.5.4.7
1.6.5 Organizational Unit (OU)	Nombre de la Unidad Organizativa de la AC Subordinada Ej. "UNIDAD DE FIRMA ELECTRONICA"	No		OID 2.5.4.11
1.6.6 Organization Identifier	Identificador "VAT(CÓDIGO_PAÍS)-IDENTIFICADOR_ORGANIZACIÓN" Ej. VATEC-1716151413001	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 del prestador, codificada de acuerdo con el algoritmo criptográfico.	Sí		
1.7.1 AlgorithmIdentifier	1.2.840.113549.1.1.1			OID 1.2.840.113549.1.1.1
1.7.1.1 Algorithm	RSA encryption	Sí		
1.7.1.2 Parameters	No aplicable	No		
1.7.2 SubjectPublicKey	Clave pública codificada de acuerdo con el algoritmo criptográfico. 4096 bits	Sí		
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 Key Identifier	Identificador de la clave del Issuer	No		
2.2 Subject Key Identifier	Presente	Sí	No	OID 2.5.29.14 (Marcado como NO crítico según EN 319412-2)
2.2.1 KeyIdentifier	Identificador de la clave del subject	Sí		
2.3 Key Usage		Sí		OID 2.5.29.15
2.3.1 Digital Signature	No seleccionado. "0"			
2.3.2 Content commintment	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"	Sí		
2.3.7 CRL Signature	Seleccionado. "1"	Sí		
2.4 Certificate Policies	Políticas de certificación / DPC	Sí	No	OID 2.5.29.32 (Marcado como NO crítico según EN 319412-2)
2.4.1 Policy Information		Sí		
2.4.1.1 Policy Identifier	2.5.29.32.0	Sí		Identificador de la política
2.4.1.2 Policy Qualifier ID	Especificación de la DPC	Sí		
2.4.1.2.1 CPS Pointer	"(https://ejemploAC.com/public/cps/)"	Sí		
2.4.1.2.2 User Notice	"(https://web.ejemplo.com/)"	Sí		
2.5 Subject Alternative Names		No	No	OID 2.5.29.17 (Marcado como NO crítico según EN 319412-2)
2.5.1 rfc822Name	info@ejemploAC.com	Sí		
2.6 cRLDistributionPoint		Sí		OID 2.5.29.31 (Marcado como NO crítico según EN 319412-2)
2.6.1 distributionPoint	"(http://crl1.example.com/arl1example.subordinada.crl)"	Sí		http (http://) IETF RFC 7230-7235 [3] or ldap (ldap://) IETF RFC 4516 [4] scheme
2.6.2 distributionPoint	"(http://crl1.example.com/arl2example.subordinada.crl)"	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	"(http://ocsp1.example.com/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	"(http://ocsp2.example.com/ocsp/)"	No		URL de acceso al OCSP (http://) IETF RFC 7230-7235 [3] or https (https://) IETF RFC 2818 [5]
2.8	**Basic Constraints**		Sí	Sí	OID 2.5.29.19
2.8.1	Subject type	cA (TRUE)	Sí		
2.8.2	Path Length Constraints	0	Sí		

REPÚBLICA DEL ECUADOR

Agencia de Regulación y Control de las Telecomunicaciones

CERTIFICADO DE VALIDACIÓN OCSP - ANEXO 8

Campo De Certificado de Validación OCSP	Autenticación y Firma	Obligatorio	Crít.	Observaciones OID 1.3.6.1.4.1.OID_Ac.2.6.1
1. Basic estructure				
1.1. Version	"2"	Sí		El literal "2" corresponde a la versión 3. X.509 v3
1.2. Serial Number	Establecido automáticamente por la AC. Número identificativo único del certificado.	Sí		No puede ser un número negativo ni 0.
1.3. Signature Algorithm	1.2.840.113549.1.1.11	Sí		
1.3.1. Algorithm	SHA-256 with RSA Signature	Sí		1.2.840.113549.1.1.11
1.3.2. Parameters	No aplicable	No		
1.4. Issuer		Sí		
1.4.1. Country Name (C)	Código del País "EC" (ISO 3166)	Sí		OID 2.5.4.6
1.4.2. Locality Name (L)	Localidad de la AC Subordinada (Ciudad) Ej. QUITO	Sí		OID 2.5.4.7
1.4.3. Organizational Unit (OU)	Nombre de la Unidad Organizativa de la AC Subordinada Ej. "UNIDAD DE FIRMA ELECTRONICA"	No		OID 2.5.4.11
1.4.4. Organization Name (O)	Nombre de la AC Subordinada "Organización"	Sí		OID 2.5.4.10
1.4.5. Common Name (CN)	Nombre de la AC Subordinada	Sí		OID 2.5.4.3
1.4.6. Organization Identifier	Identificador "VAT(CÓDIGO_PAÍS)-IDENTIFICADOR_ORGANIZACIÓN" Ej. VATEC-1716151413001	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)**	Sí		
1.5.1. Not Before	Fecha de inicio de validez	Sí		YYMMDDHHMMSSZ
1.5.2. Not After	Fecha de expiración	Sí		YYMMDDHHMMSSZ
1.6. Subject		Sí		
1.6.1. Country Name (C)	Código del País "EC" (ISO 3166)	Sí		OID 2.5.4.6
1.6.2. Locality Name (L)	Localidad de la AC Subordinada (Ciudad) Ej. QUITO	Sí		OID 2.5.4.7
1.6.3. Organizational Unit Name (OU)	Nombre de la Unidad Organizativa de la AC Subordinada Ej. "UNIDAD DE FIRMA ELECTRONICA"	Sí		OID 2.5.4.11
1.6.4. Organization Name (O)	Nombre de la AC Subordinada "Organización"	Sí		OID 2.5.4.10
1.6.5. Common Name (CN)	Nombre de la AC Subordinada	Sí		OID 2.5.4.3
1.6.6. Organization Identifier	"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
1.7. Subject Public Key Info		Sí		
1.7.1. AlgorithmIdentifier				
1.7.1.1. Algorithm	RSA encryption	Sí		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	Sí		
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	Sí	No	OID 2.5.29.14 (Marcado como NO crítico según EN 319412-2)
2.2.1. KeyIdentifier		Sí		Derivado de la clave pública
2.3. Key Usage		Sí	Sí	OID 2.5.29.15
2.3.1. Digital Signature	Seleccionado "1"	Sí		
2.3.2. Content commintment	Seleccionado "1"	Sí		
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		Sí		
2.4.1.1. Policy Identifier	1.3.6.1.4.1.oid_AC.2.6.1	Sí		Identificador de la política de la AC
2.4.1.2. Policy Qualifiers		Sí		
2.4.1.1.1 CPS URI	"(https://www.repo_example.com/dpc/)"	Sí		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 VALIDACIÓN OCSP"	Sí		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 Entidad Acreditada "info@example.com.ec"	Sí		
2.6. Extended Key Usage		Sí	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)	Sí		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)	Sí		Para validar el certificado OCSP, para no entrar en loop (debe ser NULL)
2.7. cRLDistributionPoint		Sí	No	OID 2.5.29.31 Marcado como NO crítico según EN 319412-2
2.7.1. distributionPoint	"(http://crl1.example.com/example1subordinada.crl)"	Sí		http (http://) IETF RFC 7230-7235 [3] or ldap (ldap://) IETF RFC 4516 [4] scheme
2.7.2. distributionPoint	"(http://crl2.example.com/example1subordinada.crl)"	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	"(http://www.example.com/subordinate1.crt)"	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		Sí	Sí	OID 2.5.29.19
2.10.1. cA	FALSE	Sí		