INFORME DE EJECUCIÓN DEL PROCESO DE CONSULTAS PÚBLICAS

INFORME TÉCNICO No. IT-CRDS-GR-2024-0048

PROPUESTA DE NORMA TÉCNICA PARA LA PRESTACIÓN DE LOS SERVICIOS DE INFORMACIÓN Y SERVICIOS RELACIONADOS DE LAS ENTIDADES DE CERTIFICACIÓN ACREDITADAS Y TERCEROS VINCULADOS

24 de julio de 2024

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

1. PROPUESTA DE REGULACIÓN

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

2. ANTECEDENTES

2.1. Con memorando Nro. ARCOTEL-CREG-2024-0432-M de 18 de junio de 2024 el Coordinador Técnico de Regulación remitió para conocimiento y aprobación del Director Ejecutivo de la ARCOTEL el informe Técnico No. IT-CRDS-GR-2024-0037 de 03 de junio de 2024 y la versión 2 de la Propuesta de la "NORMA TÉCNICA PARA LA PRESTACIÓN DE LOS SERVICIOS DE INFORMACIÓN Y SERVICIOS RELACIONADOS DE LAS ENTIDADES DE CERTIFICACIÓN ACREDITADAS Y TERCEROS VINCULADOS", con el propósito de que autorice el inicio del proceso de consultas públicas en aplicación de la Resolución Nro. 003-03-ARCOTEL-2015.

2.2. Mediante sumilla inserta el 24 de junio de 2023, a través del sistema de gestión documental Quipux en el memorando Nro. ARCOTEL-CREG-2024-0432-M, la Dirección Ejecutiva de la ARCOTEL autorizó el inicio del proceso de consultas públicas para la propuesta de "NORMA TÉCNICA PARA LA PRESTACIÓN DE LOS SERVICIOS DE INFORMACIÓN Y SERVICIOS RELACIONADOS DE LAS ENTIDADES DE CERTIFICACIÓN ACREDITADAS Y TERCEROS VINCULADOS".

2.3. Mediante memorando Nro. CREG-2023-0450-M de 27 de junio de 2024, la Coordinación Técnica de Regulación, dando cumplimiento a lo dispuesto por el Director Ejecutivo de la ARCOTEL, solicitó al Responsable de Comunicación Social se proceda con la publicación de la convocatoria a la audiencia pública, respecto del proyecto de regulación en consideración.

2.4. La Unidad de Comunicación Social realizó la publicación de solicitada a través del siguiente link:

https://apc.arcotel.gob.ec/preguntas/88/audiencia-publica-para-recibir-observaciones-y-comentarios-a-la-propuesta-de-norma-tecnica-para-la-prestacion-de-los-servicios-de-informacion-y-servicios-relacionados-de-las-entidades-de-certificacion-acreditadas-y-terceros-vinculados

2.5. Con memorando Nro. ARCOTEL-CREG-2024-0488-M de 11 de julio de 2024, la Coordinación Técnica de Regulación solicitó al Responsable de la Unidad de Comunicación Social, realice la publicación de las observaciones recibidas mediante correo electrónico y a través del sistema de gestión documental a la propuesta de "NORMA TÉCNICA PARA LA PRESTACIÓN DE LOS SERVICIOS DE INFORMACIÓN Y SERVICIOS RELACIONADOS DE LAS ENTIDADES DE CERTIFICACIÓN ACREDITADAS Y TERCEROS VINCULADOS".

2.6. Mediante memorando Nro. ARCOTEL-DECS-2024-0064-M de 11 de julio de 2024, el Responsable de la Unidad de Comunicación Social informó que se realizó la

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

publicación de las observaciones a la Propuesta de la "NORMA TÉCNICA PARA LA PRESTACIÓN DE LOS SERVICIOS DE INFORMACIÓN Y SERVICIOS RELACIONADOS DE LAS ENTIDADES DE CERTIFICACIÓN ACREDITADAS Y TERCEROS VINCULADOS". por parte de los interesados en el siguiente link:

https://apc.arcotel.gob.ec/preguntas/88/audiencia-publica-para-recibir-observaciones-y-comentarios-a-la-propuesta-de-norma-tecnica-para-la-prestacion-de-los-servicios-de-informacion-y-servicios-relacionados-de-las-entidades-de-certificacion-acreditadas-y-terceros-vinculados

2.7. El lunes 15 de julio de 2024, a partir de las 10h15 se efectuó la audiencia pública presencial y virtual, conforme a la convocatoria realizada de conformidad con la Resolución Nro. 003-03-ARCOTEL-2015.

3. APORTES RECIBIDOS EN EL PROCESO DE CONSULTAS PÚBLICAS

En la publicación realizada el 27 de junio de 2024 en el sitio web institucional de la ARCOTEL, en aplicación del Reglamento de Consultas Públicas (Resolución No. 003-03-ARCOTEL-2015), se otorgó el término de ocho días, es decir hasta el día 09 de julio de 2024, para que se remitan las observaciones, opiniones y comentarios a la propuesta regulatoria, por medio de correo electrónico o por escrito ingresando a través de la Unidad de Gestión Documental en la Agencia de Regulación y Control de las Telecomunicaciones.

De acuerdo con la información recibida a través del sistema de Gestión Documental Quipux y al correo electrónico institucional consulta.publica@arcotel.gob.ec, se observa que se han recibido diez (10) documentos con las opiniones, recomendaciones y comentarios, de las siguientes personas jurídicas:

- ANFAC mediante correo electrónico de 09 de julio de 2024.
- CITEC con correo electrónico de 08 de julio de 2024.
- UANATACA con oficio EBUANATACA 09- 07 -2024 mediante correo electrónico de 09 de julio de 2024
- ECLIPSOFT con correo electrónico de 09 de julio de 2024.
- FIRMA SEGURA con oficio s/n ingresado con trámite ARCOTEL-DEDA-2024-010685-E el 09 de julio de 2024.
- BID4ID con correo electrónico de 09 de julio de 2024
- SRI con correo electrónico de 09 de julio de 2024.
- SECURITY DATA S.A con correo electrónico de 08 de julio de 2024.
- DATILMEDIA con oficio S/N ingresado con trámite ARCOTEL-DEDA-2024-010655-E el 09 de julio de 2024

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

- CNT E.P con oficio CNTEP-GNARI-RG-2024-0372-O ingresado con trámite ARCOTEL-ARCOTEL-2024-0633-E el 08 de julio de 2024

4. REALIZACIÓN DE LA AUDIENCIA PÚBLICA PRESENCIAL y VIRTUAL

La audiencia pública se realizó el 15 de julio de 2024, desde las 10H15 hasta las 12H00 de las siguientes formas:

- Presencial en el Auditorio de la ex Coordinación Zonal 2 de la ARCOTEL, en la ciudad de Quito.

- Virtual a través de la plataforma Zoom mediante el enlace: https://us06web.zoom.us/j/88061357546?pwd=HwMBjI6cmMkevWrzLxp9tlDthGHQdb.1

El registro de las personas que asistieron y participaron en la audiencia de manera presencial y virtual se adjunta al presente informe como anexo.

5. ANÁLISIS DE LOS APORTES RECIBIDOS EN EL PERÍODO DE LA CONSULTA PÚBLICA

A continuación, se realiza un análisis de las observaciones recibidas a la propuesta de "NORMA TÉCNICA PARA LA PRESTACIÓN DE LOS SERVICIOS DE INFORMACIÓN Y SERVICIOS RELACIONADOS DE LAS ENTIDADES DE CERTIFICACIÓN ACREDITADAS Y TERCEROS VINCULADOS", las cuales no tienen el carácter de vinculantes para la ARCOTEL; en función del análisis técnico y su pertinencia o no, se realizan los ajustes en el proyecto de resolución que se adjunta al presente informe.

Las opiniones, recomendaciones y comentarios son los recibidos antes de la audiencia pública virtual, a través del correo consulta.publica@arcotel.gob.ec o ingresadas a la ARCOTEL, y las expresadas o reiteradas verbalmente en la audiencia pública.

El análisis por articulado, se presenta en el documento denominado "Observaciones_Firma_Electrónica.xls", adjunto al presente informe.

En cuanto a las observaciones recibidas a la estructura de cada uno de los perfiles, a fin de no duplicar o repetir el análisis, se ha realizado una clasificación por temas, el cual se presenta a continuación:

5.1. OBSERVACIONES DE FIRMA SEGURA, DATILMEDIA y SRI.

Considerando que las observaciones de las tres personas jurídicas, tienen el mismo contexto se realiza un solo análisis.

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

5.1.1. Observación a los anexos de los perfiles al atributo "Organization Identifier".

El siguiente campo de persona natural se propone en el campo obligatorio ponerlo como NO obligatorio:

- 1.4.4. Organization Identifier RUC de la AC SUB "VAT(CÓDIGO_PAÍS)-RUC" Ej. VATEC-1716151413001

Estándares internaciones dicen lo siguiente:

"4.2.3 Issuer, 4.2.3.1 - Legal person issuers:
The identity of the issuer, when the issuer is a legal person, shall contain at least the following attributes as specified in Recommendation ITU-T X.520 [6]:

- *countryName;*
- *organizationName; and*
- *commonName.*

*The identity of the issuer, when the issuer is a legal person, **should contain** the following attribute as specified in Recommendation ITU-T X.520 [6]:*

- *organizationIdentifier.".*

El siguiente campo de los perfiles se propone en el campo obligatorio ponerlo como **NO obligatorio**: 1.4.4. Organization Identifier RUC de la AC SUB "VAT(CÓDIGO_PAÍS)-RUC" Ej. VATEC-1716151413001

5.1.2. ANALISIS TÉCNICO:

Considerando la recomendación ETSI EN 319 412-2 (v2.3.1) sobre la cual se fundamenta la estructura de los perfiles de los certificados, la misma señala los términos en inglés: SHALL, SHOULD y MAY. Revisadala terminología de la ETSI[1] indica lo siguiente:

SHALL es mandatorio u obligado
SHOULD es recomendación
MAY es opcional o no de aplicar

En este sentido, para el campo OID "Organization Identifier" consta el término **SHOULD** pero esta redacción es extraída del documento de una versión obsoleta de la **ETSI EN 319 412-2 (v2.1.1) de 2016-02**, por lo que la versión vigente del documento es la **ETSI EN 319 412-2 (v2.3.1) de 2023-09** y en este documento señala que el numeral 4.2.3 "Issuer" y 4.2.3.1 Legal person issuers, en su parte pertinente señala que el atributo

[1] *Writing World Class Standards, The technical content of the standard – How to write good requirements, pag. 19*

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

OrganizationIdentifier "deberá" contener una identificación de la organización emisora del certificado diferente del nombre de la organización, está descrito con el término **Shall** el cual es mandatorio u obligatorio, por lo que revisando en la RFC 5280[2] que está basado el documento de la ETSI en la sección **4.1.2.4 "Issuer",** especifica el conjunto de atributos que deben estar preparados para recibir, de lo que no figura como mandatorio el atributo "***OrganizationIdentifier",*** en este sentido se acoge recomendación cambiando **"No obligatorio".**

5.2. OBSERVACIONES DE FIRMA SEGURA Y DATIL MEDIA.

5.2.1. Observación a los anexos de los perfiles al atributo "Access Description".

El siguiente campo de persona natural se propone en el campo obligatorio ponerlo NO Obligatorio:

2.8.2. Access Description, que abarca tanto:
a) 2.8.2.1. Access Method y,
b) 2.8.2.1.1 Access Location

Estandares internaciones dicen lo siguiente 4.4 IETF RFC 5280 internet certificate extensions
"4.4.1 Authority Information Access
The Authority Information Access extension shall be present.

The Authority Information Access extension shall include an accessMethod OID, id-ad-caIssuers, with an accessLocation value specifying at least one access location of a valid CA certificate of the issuing CA. At least one access Location shall use the http (http:// IETF RFC 7230-7235 [3] scheme or https (https://IETF RFC 2818 [5] scheme.

If the certificate does not include any access location of an OCSP responder as specified in clause 4.4.1, then the certificate shall include a CRL distribution point extension. (ETSI) Debido que el Shall si es mandatorio existe una exlusión en el 4.3.11 (ETSI EN 319 412-2)"

5.2.2. ANALISIS TÉCNICO:

Para el atributo especificado en el numeral **4.4.1 "Authority Information Access"** la ETSI EN 319 412-2 (v2.3.1) señala el término **"SHALL include"**, lo cual implica que es mandatorio u obligatorio que debe contener la extensión de acceso a la información de la Autoridad de Certificación y que incluirá un OID de método de acceso, **id-ad-caIssuers**, con un valor de ubicación de acceso que especifique al menos una ubicación de acceso de un certificado de la AC emisora.

[2] *https://datatracker.ietf.org/doc/html/rfc5280#section-4.1.2.4*

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

En el numeral 4**.3.11 "CRL distribution points"** presenta una exclusión que señala si el certificado no incluye ninguna ubicación de acceso de un respondedor OCSP como se especifica en la cláusula 4.4.1, entonces el certificado incluirá una extensión de punto de distribución de CRL.

En este sentido se acepta la recomendación de modificar a **"No obligatorio"** los numerales contenidos dentro del **2.8.2 "Access Description"** en todos los perfiles de los certificados.

5.2.3. <u>Observación a los anexos de los perfiles AC Raíz (ROOT) referente a la Validez del certificado:</u>

El siguiente campo de persona natural se encuentra obligatorio:
1.5 Validity (Se sujetará a la vigencia de la Acreditación)

Se sugiere atar la validez de los certificados a los estándares internacionales, más no a la vigencia de la acreditación, por el desfase que esto podría ocasionar.

5.2.4. ANALISIS TÉCNICO:

La vigencia tecnológica de la PKI no puede estar atado a la vigencia de la Acreditación que se le otorga a las Entidades de Certificación Acreditadas, esto limitaría la emisión de certificados..

Para una Ac raíz, que es la jerarquía de la PKI, la vigencia de los certificados que emite debe ser más larga que de las AC Subordinada. Es importante que una AC raíz mantenga una vigencia suficientemente larga para garantizar la estabilidad y la continuidad de la infraestructura PKI, ya que todos los certificados emitidos por las AC Subordinadas dependen de la confianza en la AC raíz. Sin embargo, es fundamental que la AC raíz también tenga mecanismos robustos para la revocación y la gestión de certificados en caso de compromiso o necesidad de actualización antes del vencimiento planificado, por lo cual se elimina la recomendación..

5.2.5. <u>Observación a los anexos de los perfiles referente al atributo "Authority Key Identifier":</u>

El siguiente campo de persona natural se propone en el campo obligatorio ponerlo como NO OBLIGATORIO:

2.1 Authority Key Identifier 2.1.1 Key Identifier

De acuerdo con la RFC 5280: *"The keyIdentifier field of the authorityKeyIdentifier extension MUST be included in all certificates generated by conforming CAs to facilitate certification path construction. There is one exception; where a CA distributes its public key in the form of a "self-signed" certificate, the authority key identifier MAY be omitted.".*

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 siguiente campo se propone en el campo obligatorio ponerlo como **NO OBLIGATORIO** *"2.1 Authority Key Identifier 2.1.1 Key Identifier."*

5.2.6. ANALISIS TÉCNICO:

El análisis se realiza de manera general con otra observación presentada al anexo 7 que habla del mismo punto.

La extensión del identificador de clave de autoridad **4.3.1 "Authority key Identifier"** descrito en la **ETSI EN 319 412-2 (v2.3.1)** señala el término **"SHALL be"** que deberá estar presente y contener un identificador de clave para la clave pública de la CA emisora.

Por lo que **SHALL** es un término mandatorio u obligado, pero en la RFC 5280 señala una excepción; cuando una CA distribuye su clave pública en forma de un certificado **"autofirmado"**, **PUEDE omitirse** el identificador de clave de autoridad"; por lo que siempre y cuando se cumpla esta condición puede omitirse el **"Authority key Identifier",** se acepta la recomendación se cambia a **"No obligatorio".**

En este sentido, se aclara que siempre y cuando el certificado sea "autofirmado" puede no incluirse este atributo, por lo que se cambia a **"No obligatorio",** la extensión Authority Key Identifier.

5.2.7. <u>Observación a los anexos de los perfiles referente al atributo "Certificate Policies":</u>

2.4 Certificate Policies-2.4.1, Policy Information-2.4.1.1, Policy Identifier-2.4.1.2 Policy Qualifier
ID-2.4.1.2.1 CPS
Pointer-2.4.1.2.2 User Notice

De acuerdo con la RFC 5280: 4.2.1.4. Certificate Policies.

"The certificate policies extension contains a sequence of one or more policy information terms, each of which consists of an object identifier (OID) and optional qualifiers.".

La propuesta es poner como no obligatorio dado que la norma no expresa puntualmente como un requisito obligatorio.

El siguiente campo de persona natural se propone en el campo obligatorio ponerlo como NO OBLIGATORIO:

2.4 Certificate Policies-2.4.1 Policy Information-2.4.1.1 Policy Identifier-2.4.1.2 Policy Qualifier
ID-2.4.1.2.1 CPS
Pointer-2.4.1.2.2 User Notice

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

5.2.8. ANALISIS TÉCNICO:

El análisis se realiza de manera general con otra observación presentada al anexo 7 que habla del mismo punto.

La extensión del identificador de las políticas de certificado **4.3.3 "Certificate policies**" descrito en la **ETSI EN 319 412-2 (v2.3.1)** señala el término **"SHALL be"** que deberá estar presente y contener el identificador de al menos una política de certificado que refleje las prácticas y procedimientos emprendidos por la CA.

Por lo que **SHALL** es un término mandatorio u obligado, razón por la cual no se acoge recomendación.

5.2.9. <u>Observación a los anexos de los perfiles referente al atributo "Subject Alternative Name":</u>

2.5 Subject Alternative Names:

2.5.1 rfc822Name
4.3.5 Subject alternative name

This extension shall not be marked critical. (De acuerdo con la etsi no debería ser marcado como crítico ni tampoco menciona como campo obligatorio)

El siguiente campo de persona natural se propone en el campo obligatorio ponerlo como **NO OBLIGATORIO:**

2.5 Subject Alternative Names: 2.5.1 rfc822Name

5.2.10. ANALISIS TÉCNICO:

El análisis se realiza de manera general con otra observación presentada al anexo 7 que habla del mismo punto.

Si bien es cierto lo descrito en la **ETSI EN 319 412-2 (v2.3.1)** respecto del atributo **4.3.5 "Subject alternative name"** que señala que esta extensión no debe ser marcada como crítica, y no señala sobre que debe ser obligatorio.

En los perfiles que se encuentran propuestos sobre esta extensión, si se encuentra como **"No obligatorio",** pero la extensión **2.5.1. "rfc822Name"** se encuentra como **"obligatoria"** dado que en la RFC 5280 en el numeral **4.2.1.6** señala en su parte pertinente que cuando la extensión sujetAltName contiene una dirección de correo de Internet, la dirección **DEBE almacenarse en rfc822Name**. El formato de un rfc822Name es un "Buzón" como se define en la Sección 4.1.2 de [RFC2821]. Un buzón tiene el formato "Parte local@Dominio".

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

Por lo tanto, aquí utilizan el término “MUST”, mismo que es mandatorio por lo que no se acoge recomendación.

5.3. OBSERVACIONES DE NAMIRIAL-BID4ID.

5.3.1. Observaciones realizadas a los Anexos 1a, 1b, 2a, 2b, 3a, 3b, 4a, 4b, 5:

1.4.4. Organization Identifier RUC de la AC SUB “VAT(CÓDIGO_PAÍS)-RUC” Ej. VATEC-1716151413001

De acuerdo a codificación acorde la ETSI EN 319 412-1 en lugar de colocar RUC colocar “**Identificador de la organización”**

1.4.4. Organization Identifier de la AC SUB “VAT(CÓDIGO_PAÍS)-IDENTIFICADOR” Ej. VATEC-1716151413001

5.3.2. Observaciones realizadas a los Anexos 6, 7:

De acuerdo a la codificación acorde la ETSI EN 319 412-1 en lugar de colocar RUC colocar “**Identificador de la organización”**

1.4.6 “VAT(CÓDIGO_PAÍS)-IDENTIFICADOR_ORGANIZACION” Ej. VATEC-1716151413001

5.3.3. ANALISIS TÉCNICO:

Se realiza un análisis general dado que se hace referencia al mismo tipo de cambio en diferentes anexos.

El documento basado para la nomenclatura **ETSI EN 319 412-1 V1.4.4 (2021-05)** en su numeral **5.1.4 “Legal person semantics Identifier”** en su parte pertinente señala:

"VAT" for identification based on a national value added tax identification number.

En este sentido, se acepta recomendación cambiando el término **“RUC”** por **“identificador”** ya que el documento habla de identificación de la Entidad de Certificación Acreditada, por lo que se actualiza en todos los anexos este término.

5.4. OBSERVACIONES DE SRI.

5.4.1. Modificar el OID 1.3.6.1.4.1.OID_AC.3.6 para que de forma inequívoca podamos identificar el tipo de sujeto:

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

En la descripción del OID 1.3.6.1.4.1.OID_AC.3.6 en lugar de **"Campo vacío"** incluir "Tipo de sujeto(Personal natural, Persona jurídica, Contribuyente)"

5.4.2. ANALISIS TÉCNICO:

El OID que señala en la observación no es parte de los perfiles propuestos, puesto que la estructura que se presenta es en base a los estándares y mejores prácticas internacionales, por lo que no es procedente realizar ningún análisis y no se acoge observación.

5.4.3. Incluir números de versión diferentes como oid_AC.2.1.1 y oid_AC.2.2.1, entre otros, no añade valor a la distinción del tipo de documento para firma digital. De hecho, aumenta la complejidad al realizar validaciones relacionadas con cada tipo de certificado:

Se debe mantener una única versión para cada tipo de certificado, distinguiéndolos por el tipo descrito en los puntos anteriores.

5.4.4. ANALISIS TÉCNICO:

La extensión del identificador de las políticas de certificado **4.3.3 "Certificate policies**" descrito en la **ETSI EN 319 412-2 (v2.3.1)** señala el término **"SHALL be"** que deberá estar presente y contener el identificador de al menos una política de certificado que refleje las prácticas y procedimientos emprendidos por la CA.

Por lo que **SHALL** es un término mandatorio u obligado, adicionalmente la numeración es un distintivo de cada tipo de certificado por tipo de contenedor, a más del OID que identifica a la Entidad de certificación Acreditada, no se acoge recomendación.

5.4.5. Definir codificación aceptada en los certificados digitales emitidos:

La codificación debe ser UTF-8.

5.4.6. ANALISIS TÉCNICO:

La RFC 5280, señala los diferentes tipos que deben ser elegidos o seleccionados de acuerdo a cada necesidad como por ejemplo: IA5String, UTF-8, PrintableString, UTCTime.

Por lo que, de acuerdo a las políticas de uso especificado en la RFC 5280, se deberá utilizar para los perfiles, además que no se puede limitar al uso de otros tipos de codificaciones que podrían ser adoptados en futuras versiones de esta recomendación o en otras que se puedan acoger, por lo cual no se acepta recomendación.

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

5.4.7. El Arcotel como institución rectora deberá garantizar los certificados digitales emitidos por las entidades certificadoras en estructura, tipos, etc. y el estricto cumplimiento de la normativa:

Cada Entidad de Certificación de Información y Servicios Relacionados Acreditada debe remitir de forma semestral un certificado de usuario final por cada tipo para que sea validado en estructura, tipos, etc por la Arcotel.

5.4.8. ANALISIS TÉCNICO:

La observación realizada ya consta en la norma en el artículo 4 numeral 20.

5.4.9. Las instituciones validadoras requieren de certificados de prueba de todos los tipos para completar desarrollos relacionados, en este sentido, se requiere que las entidades certificadoras remitan certificados de pruebas de cada tipo para completar los desarrollos sobre los sistemas. Pueden ser enviados por la Arcotel o por las Entidades certificadoras siempre y cuando sean validados previamente por el ente Rector(Arcotel):

Definir artículo de emisión de certificados de prueba sin costo para las instituciones validadoras.

5.4.10. ANALISIS TÉCNICO:

Se debe considerar que no es posible emitir certificados de pruebas por parte de las Entidades de Certificación Acreditadas puesto que el Reglamento General a la Ley de Comercio Electrónico, Firmas y Mensajes de Datos en su artículo 18 lo prohíbe, razón por la cual no se acepta recomendación.

5.4.11. Definir hasta que fecha serán válidos los certificados digitales emitidos hasta la fecha y hasta que fecha podrán emitir certificados con la estructura anterior.

5.4.12. ANALISIS TÉCNICO:

En las disposiciones transitorias cuarta y quinta, se realizan los ajustes al proyecto de resolución.

5.4.13. Previo a la acreditación de una nueva entidad certificadora, la misma debe contar con toda la infraestructura necesaria para emisión, validación y verificación de certificados digitales. No puede iniciar operaciones una entidad certificadora que no cuente con la infraestructura necesaria para validar peticiones de instituciones validadoras que permitan verificar revocación, anulación, etc. de certificados digitales.

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

Previo a la acreditación de una nueva entidad certificadora, la misma debe contar con toda la infraestructura necesaria para emisión, validación y verificación de certificados digitales.

5.4.14. ANALISIS TÉCNICO:

Para que se acrediten como una Entidad de Certificación, debe cumplir con los requerimientos técnicos y legales especificados en la Ley de Comercio Electrónico, Firmas y Mensajes de Datos y su Reglamento general de aplicación, así como con las condiciones establecidas con la norma técnica una vez aprobada, por lo que no se acepta recomendación.

5.4.15. Es necesario establecer un mecanismo de identificación claro para las diferentes entidades de certificación. Para estandarizar, los nuevos certificados raíz y subordinados deben ser claramente identificables por estos campos, ya que son necesarios en los procesos de validación.

Los identificadores de organización(O) y el nombre de la compañía (CN) del emisor del certificado deben ser únicos e irrepetibles.

5.4.16. ANALISIS TÉCNICO:

En los anexos propuestos en los perfiles se encuentra detallado específicamente cada uno de los OID así como la descripción de cada uno de los campos que deben contener los certificados AC Raíz, AC subordinado, de Validación OCSP, de Sellado de Tiempo, y de usuarios finales, por lo qeu estaría cubierta la observación realizada.

6. CONCLUSIONES

a) La propuesta de *"NORMA PARA LA PRESTACIÓN DE LOS SERVICIOS DE INFORMACIÓN Y SERVICIOS RELACIONADOS DE LAS ENTIDADES DE CERTIFICACIÓN ACREDITADAS TERCEROS VINCULADOS",* ha sido sometida al procedimiento de consulta pública, cumpliendo con lo dispuesto en el Reglamento de Consultas Públicas aprobado con Resolución 03-03-ARCOTEL-2015 de 28 de mayo de 2015, y se realizó la audiencia pública virtual y presencial.

a) Dentro del procedimiento de consultas públicas se recibieron sin el carácter de vinculantes para la ARCOTEL, observaciones, comentarios y sugerencias al proyecto, por correo electrónico, Sistema de Gestión Documental "Quipux" y durante la audiencia pública presencial y virtual, las cuales han sido analizadas en el presente informe y en el anexo de Excel, habiéndose acogido las recomendaciones pertinentes y en función de ello, se presenta una propuesta final de resolución.

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

7. RECOMENDACIÓN

Por lo indicado, se recomienda al Coordinador Técnico de Regulación aprobar el presente informe y ponerlo en conocimiento de la Dirección Ejecutiva, conjuntamente con el proyecto de resolución para la "NORMA PARA LA PRESTACIÓN DE LOS SERVICIOS DE INFORMACIÓN Y SERVICIOS RELACIONADOS DE LAS ENTIDADES DE CERTIFICACIÓN ACREDITADAS TERCEROS VINCULADOS", con el fin de que, de considerarlo procedente y previo criterio jurídico de la Coordinación General Jurídica, se apruebe la mencionada norma técnica.

8. ANEXOS

- Proyecto de Resolución "NORMA PARA LA PRESTACIÓN DE LOS SERVICIOS DE INFORMACIÓN Y SERVICIOS RELACIONADOS DE LAS ENTIDADES DE CERTIFICACIÓN ACREDITADAS TERCEROS VINCULADOS"
- Cuadro con el análisis de las observaciones presentadas en Excel.
- Acta de ejecución de Audiencia pública presencial y virtual.
- Listado de asistentes a audiencias pública presencial y virtual.

Atentamente,

Firmado electrónicamente por:
JAIME ALFREDO BENITEZ ENRIQUEZ

Mgs. Jaime Alfredo Benítez Enríquez
DIRECTOR TÉCNICO DE REGULACIÓN DE SERVICIOS Y REDES DE TELECOMUNICACIONES

Elaborado Por:	**Revisado por:**
Firmado electrónicamente por: FABIAN MARCELO SEGOVIA TORRES **Ing. Fabián Segovia** **Analista Técnico de Regulación de Servicios y Redes de Telecomunicaciones 2**	Firmado electrónicamente por: JENNY PAULINA ZHUNIO CIFUENTES **Ing. Paulina Zhunio** **Especialista Jefe 1**
Firmado electrónicamente por: ALEX PATRICIO BECERRA CHINGAL **Ab. Alex Becerra** **Analista Jurídico de Regulación de Servicios y Redes de Telecomunicaciones 2**	

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