INFORME DE PRESENTACIÓN DE PROYECTO DE REGULACIÓN

INFORME TÉCNICO
No. IT-CRDS-GR-2024-0040

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

17 DE JUNIO 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

ÍNDICE

1. PROYECTO DE REGULACIÓN. 3
2. OBJETIVO DEL PROYECTO DE REGULACIÓN. 3
3. ANTECEDENTES. 3
4. BASE NORMATIVA. 11
5. AUTORIDAD COMPETENTE 17
6. JUSTIFICACIÓN DE OPORTUNIDAD. 18
7. CONCLUSIÓN 41
8. RECOMENDACIONES. 41
9. ANEXOS 42

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. PROYECTO 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. OBJETIVO DEL PROYECTO DE REGULACIÓN.

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 también 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 contiene campos comunes, de tal manera que puedan ser reconocidos por las aplicaciones sin ningún tipo de restricción técnica, semántica u organizativa.

3. ANTECEDENTES.

- 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. (…)*

- Con oficio Nro. ARCOTEL-ARCOTEL-2023-0168-OF de 31 de marzo de 2023, el Director Ejecutivo de la ARCOTEL señala: *"(…) me permito remitir la hoja de ruta consensuada de las Direcciones de la ARCOTEL que trabajarán en la elaboración de la normativa requerida, así como los insumos y actividades a realizar por MINTEL; con la finalidad de que una vez revisado por su autoridad se coordine las acciones necesarias para cumplir con lo dispuesto por la máxima autoridad de MINTEL.*

  Sobre el plan de acción se precisa que el mismo contemplaría las actividades y los entregables detallados en la hoja de ruta.".

- Mediante oficio Nro. MINTEL-MINTEL-2023-0260-O de 06 de abril de 2023, el Ministerio de Telecomunicaciones y de la Sociedad de la información, menciona: *"(...) se deberá ajustar los tiempos establecidos en el cronograma y realizar la generación de normativas, regulaciones, normas internas necesarias para la regulación y control de las Entidades de Certificación acreditadas en el país acorde a*

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

los estándares internacionales y mejores prácticas. Además de la consideración en agregar alguna directriz adicional basado en los estándares y mejores prácticas".

- Con oficio Nro. ARCOTEL-ARCOTEL-2023-0201-OF de 24 de abril de 2023, el Director Ejecutivo de la ARCOTEL señala: *"(…) al respecto me permito comunicar que se realizó una reunión de trabajo entre los delegados de MINTEL y ARCOTEL el día martes 18 de abril, para determinar las acciones a seguir para el cumplimiento de lo solicitado por el Ministerio a su cargo(…)".*

- Mediante oficio Nro. MINTEL-SGERC-2023-0640-O de 26 de junio de 2023, la Subsecretaria de Gobierno Electrónico y Registro Civil convoca a reunión de trabajo para el día 28 de junio de 2023 a las 13h00, en el piso 10 del MINTEL, a efectos de revisar la información solicitada en oficios anteriores así como en las reuniones mantenidas previamente.

- A través de oficio Nro. ARCOTEL-ARCOTEL-2023-0295-OF de 30 de junio de 2023, el Director Ejecutivo de la ARCOTEL remite el cronograma ajustado para la elaboración de la normativa requerida.

- Con memorando Nro. ARCOTEL-CREG-2023-0521-M de 04 de julio de 2023, el Coordinador Técnico de Regulación solicitó información a las Coordinaciones Técnicas de Control y Títulos Habilitantes.

- Mediante memorando Nro. ARCOTEL-CCON-2023-1759-M de 10 de julio de 2023, el Coordinador Técnico de Control remitió la información solicitada.

- Con memorando Nro. ARCOTEL-CCON-2023-1973-M de 07 de agosto de 2023, el Coordinador Técnico de Control remite un alcance al Memorando Nro. ARCOTEL-CCON-2023-1759-M de 10 de julio de 2023, adjuntando el Informe Técnico Nro. IT-CCDS-2023-0023 de 04 de agosto de 2023.

- Mediante memorando Nro. ARCOTEL-CTHB-2023-1886-M de 10 de agosto de 2023, la Coordinación Técnica de Título Habilitantes remite el INFORME No. IT-CTHB-EC-2023-002 y el archivo en Excel con el resumen de los tipos de certificados.

- Con oficio Nro. ARCOTEL-CREG-2023-0100-OF de 21 de agosto de 2023, la Coordinación Técnica de Regulación, solicitó a la Dirección de Asuntos Regulatorios de la Presidencia de la República emitir su pronunciamiento respecto de la exención de la elaboración del análisis de impacto regulatorio, para la creación de la normativa que viabilice el reconocimiento internacional de certificados de firma electrónica, considerando que el proyecto normativo se sujeta expresamente a lo que establece la Ley de Comercio Electrónico, Firmas 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

- Mediante 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.".*

- Con memorando Nro. ARCOTEL-CREG-2024-0038-M de 15 de enero de 2024, la Coordinación Técnica de Regulación solicitó a las distintas Coordinaciones de la ARCOTEL remitir sus observaciones y comentarios debidamente justificados, dentro del ámbito de sus competencias de la versión 0 del proyecto normativo.

  Adicionalmente, a la Coordinación General Jurídica se solicitó emita el informe jurídico sobre la autoridad competente correspondiente.

- A través de oficio Nro. ARCOTEL-CREG-2024-0010-OF de 15 de enero de 2024, la Directora Ejecutiva de la ARCOTEL solicitó al MINTEL observaciones al Proyecto de resolución e informe de la versión 0 de la "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 memorando Nros. 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, la Coordinación Zonal 5, la Coordinación General Jurídica y la Coordinación Técnica de Títulos Habilitantes respectivamente señalaron que no cuentan con observaciones al proyecto.

- Mediante memorando Nro. ARCOTEL-CCON-2024-0163-M de 23 de enero de 2024, la Coordinación Técnica de Control remitió observaciones al proyecto borrador de norma para los servicios de certificación de información.

- 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***

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

GARANTIZAR LA INTEROPERABILIDAD Y ESTANDARIZACIÓN DE LOS PROCESO ELECTRÓNICOS", debe ser 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.".* (Énfasis Agregado)

- A través oficio Nro. MINTEL-MINTEL-2024-0028-O de 30 de enero de 2024, el Ministro de Telecomunicaciones y de la Sociedad de la Información emite la respuesta con las observaciones al proyecto de resolución e informe de la versión 0 al proyecto normativo antes mencionado.

- Con oficio Nro. ARCOTEL-CREG-2024-0026-OF de 01 de febrero de 2024, la Coordinación Técnica de Regulación dio contestación al Subsecretario de Gobierno Electrónico y Registro Civil, respecto a las observaciones remitidas por el MINTEL.

- A través de oficio Nro. MINTEL-SGERC-2024-0111-O de 06 de febrero de 2024, el Subsecretario de Gobierno Electrónico y Registro Civil del MINTEL emitió sus observaciones en respuesta al oficio enviado por la Coordinadora Técnica de Regulación.

- Con memorando Nro. ARCOTEL-CREG-2024-0110-M de 09 de febrero de 2024, la Coordinación Técnica de regulación realizó varias consultas jurídicas relacionadas con la firma electrónica.

- Con memorando Nro. ARCOTEL-CJUR-2024-0137-M de 20 de febrero de 2024, la Coordinación General Jurídica señaló: remite el Criterio Jurídico No. ARCOTEL-CJDA-2024-0017 de 20 de febrero de 2024, que cuenta con la aprobación de esta Coordinación General Jurídica, que en su parte pertinente señala:

  Respecto a la pregunta 1: *"(...) En tal razón, corresponde a la Coordinación Técnica de Regulación, determinar la procedencia o no de establecer un estándar para la emisión de firmas electrónicas.".*

  Respecto a la pregunta 2: *"(…) se considera que no existe normativa expresa que pueda limitar a los usuarios la obtención de su firma electrónica únicamente a través de una atención presencial.".*

  Respecto a la pregunta 3: *"(…) sin que exista en la normativa aplicable limitante para que un usuario que ya cuenta con una firma electrónica vigente, pueda obtenerla en otra entidad de certificación acreditada.".*

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

Respecto a la pregunta 4: *"(…) Considerando la normativa citada y conforme lo dispuesto en el artículo 144, numeral 29 de la Ley Orgánica de Telecomunicaciones, la ARCOTEL tiene la atribución dada por Ley para desarrollar los mecanismos, políticas y procedimientos para auditar técnicamente la actividad de las entidades de Certificación y Servicios Relacionados Acreditadas.".*

Respecto a la pregunta 5: *"(…) correspondiendo a la Coordinación de Regulación, a través de la Dirección Técnica de Regulación de Servicios y Redes de Telecomunicaciones, dentro del ámbito de sus atribuciones y competencias determinar si procede regular condiciones específicas para la prestación del servicio de sellado de tiempo, como: modelo de operación de la autoridad de sellado de tiempo, políticas y declaraciones de prácticas de sellado de tiempo, estructura de sellado de tiempo, políticas de sellos de tiempo, entre otras."*

- Mediante oficio Nro. ARCOTEL-CREG-2024-0037-OF de 22 de febrero de 2024, la Coordinación Técnica de Regulación dio atención al Oficio Nro. MINTEL-SGERC-2024-0152-O de 20 de febrero de 2024, A través de oficio Nro. MINTEL-SGERC-2024-0174-O de 26 de febrero de 2024, el Subsecretario de Gobierno Electrónico y Registro Civil del MINTEL remitió las observaciones al proyecto normativo.

- Mediante oficio Nro. ARCOTEL-CREG-2024-0042-OF de 01 de marzo de 2024, la Coordinación Técnica de Regulación realizó una consulta al Consejo de la Judicatura sobre la pertinencia de mantener el tipo de firma como "Certificado de Persona Jurídica, Representante Legal, Miembro de Empresa o Empleado con relación de dependencia.", con relación al Acuerdo Ministerial No. 006-2015 de 27 de enero de 2015.

- Con oficio Nro. ARCOTEL-CREG-2024-0044-OF de 04 de marzo de 2024, la Coordinación Técnica de Regulación remitió la aclaración a las observaciones presentadas en el oficio Nro. MINTEL-SGERC-2024-0174-O Propuesta de "NORMA PARA LA PRESTACIÓN DE LOS SERVICIOS DE INFORMACIÓN Y SERVICIOS RELACIONADOS DE LAS ENTIDADES DE CERTIFICACIÓN ACREDITADAS Y TERCEROS VINCUALDOS".

- Mediante memorando Nro. ARCOTEL-CREG-2024-0163-M de 05 de marzo de 2024, la Coordinación Técnica de Regulación realizó la siguiente petición a la Dirección Ejecutiva: solicitó autorización para la ejecución de talleres del proyecto normativo, mismo que fue aprobado el 14 de marzo de 2024 por la Dirección Ejecutiva mediante sumilla inserta en Quipux.

- Con oficio Nro. ARCOTEL-CREG-2024-0047-OF de 11 de marzo de 2024, la Coordinación Técnica de Regulación remitió al MINTEL el nuevo cronograma de ejecución del proyecto normativo.

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 través de oficio Nro. MINTEL-SGERC-2024-0291-O de 11 de marzo de 2024, el Subsecretario de Gobierno Electrónico y Registro Civil del MINTEL, señaló: *"(…) Se ha revisado la documentación referida y se ha establecido que la misma se encuentra a conformidad con las observaciones levantadas en la mesa del trabajo del pasado 27 de febrero de 2024. (…)".*

- Con oficio Nro. MINTEL-SGERC-2024-0297-O de 13 de marzo de 2024, el Subsecretario de Gobierno Electrónico y Registro Civil del MINTEL, solicitó que se realicen los ajustes en las actividades y en los tiempos programados del último cronograma emitido, debiendo dar cumplimiento a la emisión de la referida normativa, y sin fecha de postergación, hasta el mes de julio de 2024.".

- Mediante oficio Nro. ARCOTEL-CREG-2024-0052-OF de 15 de marzo de 2024, la Coordinación Técnica de Regulación remitió el nuevo cronograma.

- Con oficios Nros. ARCOTEL-CREG-2024-0053-OF, ARCOTEL-CREG-2024-0054-OF, ARCOTEL-CREG-2024-0055-OF y ARCOTEL-CREG-2024-0056-OF de 15 de marzo de 2024, la Coordinación Técnica de Regulación realizó la socialización con los actores externos para que sea revisada y analizada la propuesta normativa en el ámbito de sus competencias, para posterior remisión de sus observaciones y aportes hasta el 26 de marzo de 2024 al correo electrónico fabian.segovia@arcotel.gob.ec.

- Con oficio Nro. Oficio-CJ-DG-2024-0515-OF de 19 de marzo de 2024, el Director General del Consejo de la Judicatura, dio atención al oficio Nro. ARCOTEL-CREG-2024-0042-OF de 01 de marzo de 2024, en el cual concluyó y recomendó que:

  "(…)

  "CONCLUSIONES:

  En virtud de todo lo hasta aquí expuesto, podemos concluir que las y los notarios son personas naturales que prestan sus servicios a la ciudadanía a través de personas que laboran bajo la modalidad de dependencia de las y los notarios, por lo cual, no se enmarcan dentro de la categoría de ´persona jurídica, representante legal o miembro de empresa´

  Bajo esta lógica, es preciso señalar que, en lo referente a la facturación electrónica, las y los notarios delegan esta responsabilidad de emisión de facturas, comprobantes de retención y documentos complementarios a las y los trabajadores que prestan sus servicios bajo relación de dependencia; y por ello, existe la necesidad de regular las responsabilidades de quienes usan la firma electrónica de las y los notarios en todos sus ámbitos de aplicación, a fin de que se confieran las debidas responsabilidades de buen uso de acuerdo a la normativa vigente y una actuación con debida diligencia, con la toma de medidas de seguridad informática

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

necesarias, para mantener la firma electrónica bajo su estricto control y evitar toda utilización no autorizada;

RECOMENDACIÓN:

Conforme el análisis realizado tanto por la Dirección Nacional de Asesoría y Normativa así como por la Dirección Nacional de Tecnologías de la Información y Comunicaciones, y con base en todo lo antes expuesto, se recomienda a la Agencia de Regulación y Control de las Telecomunicaciones, que considere e incluya en el proyecto normativo que se encuentra realizando para regular a las Entidades de Certificación de Información y Servicios Relacionados Acreditadas, en el tipo de certificado del literal (a), la figura de ´empleado en relación de dependencia en el numeral´, bajo el siguiente detalle:

1. *Certificado de Persona Natural o Física, o Empleado en Relación de Dependencia".".*

- Con oficio Nro. MINTEL-SGERC-2024-0444-O de 18 de abril de 2024, la Subsecretaria de Gobierno Electrónico y Registro Civil solicitó los avances del cronograma: *"(…) remitir a esta Cartera de Estado los avances del cronograma, considerando que, de acuerdo al corte actual, ya se tuvo que cumplir con la realización de los talleres con las 13 entidades certificadoras acreditadas por su representada, con el objeto de la presentación de la norma técnica preliminar y observaciones respectivas a la misma.".*

- Mediante oficio Nro. ARCOTEL-CREG-2024-0077-OF de 01 de mayo de 2024, la Coordinación Técnica de Regulación dio respuesta a lo solicitado: *"(…) En este contexto, se informa que se cumplió con el HITO 6 del cronograma respecto al desarrollo de talleres, los cuales fueron en las instalaciones del ARCOTEL en el piso 12 del edificio Zeus ubicado en la Diego de Almagro y Alpallana.".*

- Con oficio Nro. MINTEL-SGERC-2024-0541-O de 27 de mayo de 2024, la Subsecretaria de Gobierno Electrónico y Registro Civil solicitó: *"(…) Se solicita remitir a esta Cartera de Estado los avances del cronograma en el HITO 7 y 8, considerando que, de acuerdo al corte actual, ya está por fenecer a finales del mes de mayo el HITO 8 "REVISIÓN INTERNA" por su representada.*

  Adicionalmente, se solicita una reunión con el equipo de trabajo para la revisión del estatus de la Norma Técnica y los cumplimientos de los tiempos para llegar a su publicación oficial, la misma que será en las oficinas de MINTEL, el viernes 31 de mayo de 2024, a las 11h00.".

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

- Mediante oficio Nro. ARCOTEL-CREG-2024-0098-OF de 28 de mayo de 2024, la Coordinación Técnica de Regulación señaló: *"(…)En este contexto, como avances del cronograma establecido se tiene:*

    - *Se ha realizado el cumplimiento del HITO 7 que corresponde a la "Elaboración de propuesta normativa Versión 2 (V.2.) e Informe", lo cual se expondrá en la reunión convocada para el 31 de mayo de 2024, por parte del ingeniero Fabián Segovia.*
    - *Con respecto al HITO 8 "Revisión interna" se prevé finalizar de acuerdo a lo programado, el día viernes 31 de mayo de 2024;*

    Cabe mencionar, que se está dando cumplimiento al cronograma respectivo, y se continuará con el siguiente HITO 9 "Aprobación de la Coordinación Técnica de Regulación", en el periodo del 03 al 06 de junio de 2024.".

    - Mediante memorando Nro. ARCOTEL-CRDS-2024-0113-M de 03 de junio de 2024, la Dirección Técnica de Regulación de Servicios y Redes de Telecomunicaciones remitió a la Coordinación Técnica de Regulación el informe técnico Nro. IT-CRDS-GR-2024-0037 de 03 de junio de 2024 y el proyecto de Resolución versión 2 (v.2) para su conocimiento y aprobación, mismo que mediante sumilla inserta señaló: *"Revisión, análisis y actualización, considerando las recomendaciones del Oficio Nro. MINTEL-SGERC-2024-0581-O y su Alcance.".*

    - Con oficio Nro. MINTEL-SGERC-2024-0581-O de 05 de junio de 2024, la Subsecretaria de Gobierno Electrónico y Registro Civil del MINTEL, remitió a la Dirección Ejecutiva de la ARCOTEL el resumen de los puntos tratados en la reunión del 31 de mayo de 2024, que se mantuvo en las instalaciones del MINTEL.

    - A través de oficio Nro. MINTEL-SGERC-2024-0585-O de 06 de junio de 2024, la Subsecretaria de Gobierno Electrónico y Registro Civil del MINTEL, remitió a la Dirección Ejecutiva de la ARCOTEL un alcance al oficio Nro. MINTEL-SGERC-2024-0581-O de 05 de junio de 2024, en el cual presenta las observaciones al proyecto normativo y al informe técnico.

    - Con oficio Nro. ARCOTEL-CREG-2024-0105-OF de 11 de junio de 2024, la Coordinación Técnica de Regulación remitió a la Subsecretaria de Gobierno Electrónico y Registro Civil del MINTEL el proyecto de informe, proyecto de resolución y anexos en base a las observaciones mencionadas, así como una actualización del cronograma por las actividades adicionales de revisión que ha realizado el MINTEL al borrador de informe y proyecto de resolución v.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

- A través de oficio Nro. MINTEL-SGERC-2024-0620-O de 12 de junio de 2024, la Subsecretaria de Gobierno Electrónico y Registro Civil del MINTEL remitió a la Coordinación Técnica de Regulación observaciones complementarias a los borradores del proyecto normativo y al informe técnico, así como solicitó realizar una mesa técnica el 17 de junio de 2024 en sus instalaciones.

4. BASE NORMATIVA.

4.1 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.".*

4.2 El Código Orgánico Administrativo 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.".

4.3 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

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

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 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.".

4.4 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

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

electrónicos, a través de redes de información, incluido el comercio electrónico, la protección a los usuarios de estos sistemas, y el reconocimiento de los certificados de firma electrónica entre los países suscriptores.". (Énfasis agregado)

"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.".

4.5 El Reglamento General a la Ley Orgánica 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.".

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

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

4.6 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.".

4.7 El Reglamento General a la Ley Orgánica de la Transformación Digital y Audiovisual, establece:

"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

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

y Audiovisual, las entidades del sector público y privado 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.".

4.8 La Ley Orgánica para la 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;

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) 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

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.".

4.9 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.".

4.10 Con Acuerdo Ministerial Nro. 181 de 15 de septiembre de 2011, a través del cual 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 y determinó los campos obligatorios de dichos tipos de certificados y números identificadores de campos u OID.

4.11 Mediante Acuerdo Ministerial Nro. 006-2015 de 27 de enero de 2015, el Ministerio de Telecomunicaciones y de la Sociedad de la Información, acuerda

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

reformar 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.

4.12 Con Acuerdo Ministerial Nro. 012-2016 de 23 de mayo de 2016, con el cual 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) de los acápites 1.2.1 y 1.2.2 del artículo1, suprimiendo el tipo de certificado con la figura de Funcionario Público.

5. AUTORIDAD COMPETENTE

La Constitución de la República del Ecuador en el artículo 226 determina: *"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."*.

La Ley Orgánica de Telecomunicaciones en su artículo 144, establece como parte de las competencias de la Agencia de Regulación y Control de las Telecomunicaciones (ARCOTEL) las siguientes: "*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 cumpla 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.".*

El Reglamento General a la Ley Orgánica de Telecomunicaciones, en el artículo 6, señala: *"(…) La máxima autoridad de dirección y regulación de la ARCOTEL es el Directorio; y, la máxima autoridad con facultad ejecutiva, de administración y de regulación es el Director Ejecutivo, quien ejerce la representación legal, judicial y extrajudicial de la ARCOTEL; y, será en consecuencia el responsable de la gestión administrativa, económica, técnica regulatoria, en los casos previstos en la LOT, y operativa. (…)"*. (Énfasis agregado)

Con memorando Nro. ARCOTEL-CJUR-2024-0084-M de 26 de enero de 2024, la Coordinación General Jurídica remite el Informe Jurídico No. ARCOTEL-CJDA-2024-0009 de 26 de enero de 2024, que concluye: *"(…)En consideración de los antecedentes, competencia y análisis expuestos, la Dirección de Asesoría Jurídica, concluye que la propuesta (…) debe ser 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*

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 Ley Orgánica de Telecomunicaciones y el procedimiento determinado en el Reglamento de Consultas Públicas.".

En virtud de lo mencionado se puede colegir que la autoridad competente para la aprobación de la propuesta regulatoria denominada *"NORMA TÉCNICA PARA LA PRESTACIÓN DE LOS SERVICIOS DE INFORMACIÓN Y SERVICIOS RELACIONADOS DE LAS ENTIDADES DE CERTIFICACIÓN ACREDITADAS Y TERCEROS VINCULADOS"*, es el Director Ejecutivo de la Agencia de Regulación y Control de las Telecomunicaciones.

6. JUSTIFICACIÓN DE OPORTUNIDAD.

La Constitución de la República del Ecuador en el artículo 226 determina que 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.

La Ley Orgánica de Telecomunicaciones en su artículo 144, determina que le corresponde a la Agencia de Regulación y Control de las Telecomunicaciones, 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; así también la Ley ibídem en la Disposición Final Cuarta, determina que la Agencia de Regulación y Control de las Telecomunicaciones ejercerá las funciones de regulación, control y administración atribuidas al Consejo Nacional de Telecomunicaciones, en la Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos, su Reglamento General y demás normativa.

La Ley de Comercio Electrónico, Firmas y Mensajes de Datos, en su artículo 28, determina que el Consejo Nacional de Telecomunicaciones dictará el reglamento para la aplicación del reconocimiento internacional de certificados de firma electrónica emitidos por entidades de certificación extranjeras, así también la Ley Ibídem en el artículo 37 establece que 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, la Ley Orgánica de Telecomunicaciones en la Disposición Final Cuarta determina que la ARCOTEL 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.

Adicionalmente la Ley de Comercio Electrónico, Firmas y Mensajes de Datos en su artículo 28, Reconocimiento internacional de certificados de firma electrónica, establece que el ex Consejo Nacional de Telecomunicaciones hoy ARCOTEL, dictará el reglamento correspondiente para la aplicación de este artículo; y en su Disposición

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

general Segunda dispone que la actividad de sellado de tiempo deberá ser acreditado técnicamente por el ex Consejo Nacional de Telecomunicaciones hoy ARCOTEL.

En este sentido, mediante oficio Nro. MINTEL-MINTEL-2023-0181-O de 15 de marzo de 2023, el Ministerio de Telecomunicaciones y Sociedad de la Información (MINTEL), solicitó a la 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.

Para lograr una armonización y facilitar las transacciones comerciales, es necesario contar con principios generales para regular a través de una Norma Técnica, el esquema de estructura de Identificadores de objeto (OID) para los perfiles de los certificados de información y servicios relacionados que emiten las Entidades de Certificación de Información y Servicios Relacionados y la vinculación en dicha norma para los Terceros Vinculados. Los identificadores de Objeto - OID aplicados correctamente, son la base de toda la interoperabilidad y estandarización de los procesos electrónicos de las Instituciones y Organismos del sector público y en el resto de los sectores de la sociedad, respecto de los certificados de información y servicios relacionados.

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

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

6.1 ENTIDADES DE CERTIFICACIÓN DE INFORMACIÓN Y SERVICIOS RELACIONADOS ACREDITADAS Y TERCEROS VINCULADOS

A continuación se detalla, las Entidades de Certificación de Información y Servicios Relacionados Acreditadas y sus Terceros Vinculados.

1) ALPHA TECHNOLOGIES CIA. LTDA. (Vigencia 22/11/2032)
2) ANFAC AUTORIDAD DE CERTIFICACION ECUADOR C.A (Vigencia 24/11/2026)

- **TERCEROS VINCULADOS:**
  - SANCHEZ DEL HIERRO ESTEBAN
  - ABITMEDIA S.A.S.
  - COOPERATIVA DE AHORRO Y CRÉDITO ALIANZA DEL VALLE LTDA.

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

- QUIZHPE QUIZHPE CHRISTIAN AMABLE

3) ARGOSDATA CERTIFICACIÓN DE INFORMACIÓN Y SERVICIOS RELACIONADOS S.A.S (Vigencia 19/10/2031)
4) BANCO CENTRAL DEL ECUADOR (Vigencia 05/11/2028)
   - **TERCEROS VINCULADOS:**
     - DIRECCION GENERAL DE REGISTRO CIVIL, IDENTIFICACION Y CEDULACION.
     - LATINUS-E-PROFESSIONAL BUSINESS S.A
     - DESARROLLO E INTEGRACION DE PROCESOS DIGITALES SODIG S.A.
5) CONSEJO DE LA JUDICATURA (Vigencia 05/09/2024)
6) CORPNEWBEST CIA. LTDA. (Vigencia 13/07/2033)
7) DATILMEDIA S.A. (Vigencia 30/08/2031)
   - **TERCEROS VINCULADOS:**
     - SERVICIOS INTEGRADOS DE COMUNICACIÓN SERIDEC S.A.
     - CARRERA OLMEDO BIENES Y SERVICIOS OLBIENSER CIA. LTDA.
     - DEVLABCOM S.A.
     - DEVCOMM S.A.S.
8) DIRECCIÓN GENERAL DE REGISTRO CIVIL, IDENTIFICACIÓN Y CEDULACIÓN (Vigencia 10/02/2031)
9) ECLIPSOFT S.A. (Vigencia 05/07/2031)
10) FIRMASEGURA (Vigencia 13/12/2033)
11) LAZZATE CIA. LTDA. (Vigencia 24/05/2032)
12) SECURITY DATA SEGURIDAD EN DATOS Y FIRMA DIGITAL S.A. (Vigencia 24/12/2030)
    - **TERCEROS VINCULADOS:**
      - ENTERPRISEPLUS S.A.
      - EMPRENDIMIENTOS TEGNOLOGICOS EMPRENDOLABS S.A.
      - CORPORACIÓN CONFIABLE S.A.
      - CONSULTORA FAUSTO AVILA ASOCIADOS CIA. LTDA.
      - BANCO GENERAL RUMIÑAHUI S.A.
      - RIZK TECHOLOGY S.A.
13) UANATACA ECUADOR S.A. (Vigencia 15/03/2031)
    - **TERCEROS VINCULADOS:**
      - SEPROTEICO S.A.
      - HAZLOFACIL S.A.S.
      - MOVILBANK CIA. LTDA.

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

- METODOS AVANZADOS INDUSTRIALES COGNOS CIA. LTDA.
- BEST BUSSISNES PLUS THEBEST S.A.
- EC593 DATA S.A.S.
- NEXTI BUSINESS SOLUTIONS S.A.
- COUNTELSEG PROFESSIONAL SOLUTIONS S.A.S.
- CREDIGESTION S.A.
- MOBILEXTREME S.A.S.
- UNO DOS TRES FÁCIL UDTFÁCIL S.A.
- EVICERTIA DEL ECUADOR CÍA LTDA
- SEGURIDAD INFORMATICA CERFIM S.A.
- LINCKA S.A.
- KA-SI GRUPOEMPRESARIAL S.A.S.
- TECSINFO S.A.
- ZUKALO S.A.
- EFILE EFIDOC S.A.
- EQ-PAY S.A.S.

Estas son las entidades de Certificación de Información y Servicios Relacionados Acreditadas y sus Terceros Vinculados que se encuentra vigentes y registrados en la Agencia de Regulación y Control de las Telecomunicaciones, que se encuentran publicadas en la página web institucional de enero a febrero de 2024.

6.2 ASPECTOS TÉCNICOS DE LOS CERTIFICADOS DE FIRMAS ELECTRÓNICAS

Conforme las normas internacionales[1], existe tres tipos distintos de representación de árbol de jerarquía de Autoridades de Certificación AC y Autoridades de Registro AR conforme los OID, definidos de acuerdo a una asignación jerárquica, que garantiza la unicidad de los mismos, definidos por la ISO (Organización Internacional de Estandarización o International Organization for Standardization) y la ITU (Unión Internacional de Telecomunicaciones o International Telecommunication Union):

1. Nodo raíz 0: nodo restringido para la UIT-T: Sector de telecomunicaciones de la UIT.

2. Nodo raíz 1: nodo de la ISO.

3. Nodo raíz 2: nodo que junta ISO-ITU y donde se utiliza los códigos asignados para país.

[1] Basado en la Norma ISO/IEC 8824-1.

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

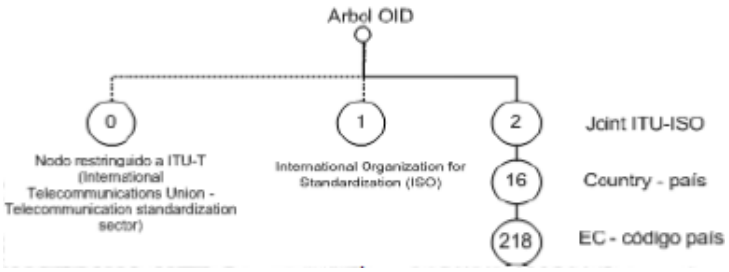

Ilustración 1. Árbol OID[2]

La utilidad de poseer un OID está basada en el reconocimiento de unicidad internacional de los objetos de determinada organización y en la oportunidad de poseer mecanismos de registro y control interno, por lo que conforme lo indicado, en Ecuador cada Entidad de Certificación de Información y Servicios Relacionados con la firma electrónica ha gestionado por sí misma el registro de un OID propio y único en las agencias registradoras operativas a nivel mundial (IDENTIFICADORES OBJETO SEGÚN NORMALIZACIÓN INTERNACIONAL DE IANA (Internet Assigned Numbers Authority)).

Por lo tanto conforme el nodo raíz 1 de la ISO, se tiene la siguiente estructura para el OID:

1.3.6.1.4.1.OID_AC.n, donde OID_AC es el OID propio y único asignado a la Entidad de Certificación de Información y Servicios Relacionados con la firma electrónica y *n* es el identificador asignado para los certificados de información y servicios relacionados conforme lo detallado en el literal siguiente.

6.2.1 Esquema de los perfiles de los certificados emitidos por las Entidades de Certificación de Información y Servicios Relacionados y sus Terceros Vinculados:

Los perfiles de certificados de firma electrónica son una forma de categorizar los certificados digitales según su propósito y alcance de uso. Estos perfiles definen las características de los certificados, lo que ayuda a garantizar su interoperabilidad acorde a los estándares y recomendaciones internacionales, razón por la cual se propone en el proyecto normativo los tipos de certificados y conforme a las mejores prácticas internacionales, que deberían emitir las Entidades de Certificación de Información y Servicios Relacionados y sus Terceros Vinculados, diferenciando cada perfil por el tipo de contenedor, los cuales se clasifican de la siguiente manera:

a) Certificados en software o archivo p.12 - (PKCS #12).
b) Certificados en Dispositivos Seguros de Creación de Firma (DSCF): Certificados en Dispositivos Criptográficos Seguros, Certificados Remotos o en nube (HSM) y Certificados en Tarjeta Criptográfica.

[2] Norma ISO/IEC 8824-1 y Documento OID - UIT

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 almacenamiento debe estar de acuerdo a las políticas de certificados, manteniendo niveles y estándares de seguridad.

El servicio de consulta de los Certificados estará a disposición de los usuarios en la página web de las Entidades de Certificación de Información y Servicios Relacionados por número de serie.

En este sentido, se desprende los distintos perfiles, mismos que se encuentran como anexos en el proyecto de resolución detallados de la siguiente manera:

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 / 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 para Autoridad de Certificación Raíz – Anexo 6

7. Certificado para Autoridad de Certificación Subordinada – Anexo 7

8. Certificado de Validación OCSP – Anexo 8

6.2.2 Recomendaciones y Estándares Internacionales:

Para la prestación de los servicios de certificación de información y servicios relacionados, las Entidades de Certificación de Información y Servicios Relacionados Acreditadas deberán observar los aspectos técnicos y de seguridad establecidos en los estándares internacionales y normativa vigente aplicable.

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

Los certificados que permiten su verificación, son herramientas fundamentales a la hora de otorgar validez a los documentos electrónicos. Por ello, la tecnología que viabiliza su utilización requiere de especial cuidado y atención.

Este cuidado se vincula fundamentalmente a la utilización de estándares tecnológicos basados en normas y protocolos internacionalmente aceptados.

Esto último asegura no sólo el correcto funcionamiento de Infraestructura de Firma Electrónica, sino también la interoperabilidad de las aplicaciones entre Entidades de Certificación Acreditadas nacionales con las infraestructuras de otros países.

Frente a cualquier transacción que involucre el uso de firma electrónica o de un certificado digital, la adopción de estándares tecnológicos internacionalmente aceptados permite asegurar un proceso efectivo de verificación de dichas firmas, otorgando seguridad técnica y legal a las transacciones electrónicas.

En este contexto, se propone el uso de los siguientes estándares tecnológicos:

- 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).
- Generación de las claves: RSA.

ITU–T RECOMMENDATION X.509 | ISO/IEC 9594–8

Recomendación / Estándar Internacional que establece el Marco para Certificados de Clave Pública (PKI) y Certificados de Atributo (PMI). Incluye la especificación de los objetos de datos usados para representar los certificados en sí mismos, tanto como la información sobre la revocación de los emitidos, a través de la lista de los revocados. La especificación define la base fundamental desde la cual se puede construir una infraestructura de clave pública completa con sus especificaciones y algunos componentes críticos de dicha infraestructura, aunque no lo hace en su totalidad.

La Versión 3 del X.509 amplía la funcionalidad del estándar. Define las extensiones del certificado, lo cual permite que una organización pueda establecer sus propias extensiones para contener información específica de su entorno de operación, así como también las extensiones en la Lista de Certificados Revocados: CRL (por su sigla en

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

inglés). De igual modo, define también los objetos de información para mantener los objetos PKI en el Directorio y cómo realizar la comparación entre los valores actuales y los almacenados. Igualmente, brinda los servicios de autenticación para el Directorio y los usuarios. La información almacenada en el Directorio, más conocida por su sigla en inglés: DIB (Directory Information Base/Base de Información del Directorio), es generalmente utilizada para facilitar las comunicaciones entre objetos tales como entidades–aplicaciones, terminales, personas y listas de distribución.

RFC 6960 – X.509 Infraestructura de Clave Pública Internet. PKI Protocolo en línea del Estado del Certificado – OCSP *(Online Certificate Status Protocol)*

Este documento especifica el protocolo para determinar el "estado actual" de un certificado digital, sin requerir la lista de certificados revocados (CRL) en la infraestructura PKI. Los mecanismos adicionales que direccionan los requerimientos operacionales no son especificados en este documento.

El Protocolo en línea de Estado del Certificado (OCSP) permite a las aplicaciones determinar el estado (revocación) de un certificado identificado. El OCSP puede ser usado para satisfacer algunos de los requerimientos operacionales de proveer en forma más oportuna la información del "estado" de la revocación que la que es posible con las CRL y puede ser usado para obtener información adicional del estado de un certificado. Un cliente de OCSP emite un requerimiento de estado a un servidor OCSP y supedita la aceptación del certificado hasta que el servidor OCSP le provea la respuesta.

Este protocolo especifica qué dato necesita ser intercambiado entre una aplicación que comprueba el estado de un certificado y un servidor que provee dicha información de estado.

FIPS 140-2 (Federal Information Processing Standards)

FIPS 140–2 es un estándar emitido por el NIST (National Institute of Standards and Technology), con el objetivo de establecer los requerimientos de seguridad que deben cumplir los módulos criptográficos utilizados para la protección de información sensible. Este estándar fue emitido con el fin de coordinar los requerimientos que deben ser observados por los departamentos y agencias gubernamentales de los Estados Unidos, cuando utilizan dispositivos criptográficos. FIPS es un acrónimo de "Federal Information Processing Standard", es decir: Estándar Federal para el Procesamiento de Información. El estándar FIPS 140–2 se refiere tanto a componentes de hardware como de software y comprende también otros aspectos, como por ejemplo, la condiciones que debe cumplir la documentación. Remplaza al FIPS 140–1, emitido previamente también por el NIST.

Hoy en día, este estándar es aceptado internacionalmente como guía para la incorporación de dispositivos criptográficos en instalaciones seguras, ya que es posible validar cada producto a través de certificados en los que se especifica el nombre exacto del módulo, el hardware, el software, la firma y los números de versión de cada componente sujeto a validación.

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 estándar mencionado propone un esquema incremental de exigencias de seguridad, basado en 4 niveles que cubren una amplia gama de aplicaciones y ambientes en los que se emplean módulos criptográficos. Estas exigencias resguardan áreas vinculadas al diseño seguro y la implementación adecuada de un módulo criptográfico y abarcan aspectos tales como especificaciones técnicas, características de los puertos e interfaces, roles y servicios, mecanismos de autenticación, condiciones de seguridad física y del ambiente operacional y aspectos vinculados a la gestión de claves criptográficas, la compatibilidad y la protección contra interferencias electromagnéticas, así como autoevaluaciones y cuestiones vinculadas a la mitigación de otros ataques. Los requisitos exigidos para cada nivel se suman a los correspondientes del anterior.

Los cuatro niveles establecidos por el estándar FIPS 140–2 contienen las siguientes prescripciones:

FIPS 140–2 nivel 1: Es el de menor exigencia ya que impone una serie acotada de requerimientos. No establece estipulaciones específicas respecto a los mecanismos de seguridad física, más allá de un mínimo de condiciones vinculadas al proceso de producción. Permite que los componentes de software y el firmware sean ejecutados en un sistema de propósito general que emplea un sistema operativo no evaluado. La utilización de un dispositivo que alcanza este nivel se aconseja sólo cuando no existen otros controles, tales como los físicos, los de red y los administrativos, o cuando éstos sean muy limitados.

FIPS 140–2 nivel 2: Agrega requerimientos en materia de seguridad, entre los cuales se encuentran la inclusión de instancias que permitan la generación de evidencia frente a manipulaciones y la autenticación, en base a roles previamente asignados. En este último caso, el módulo criptográfico debe verificar la autorización de un operador para asumir un rol específico y acceder a un determinado conjunto de servicios. En este nivel se permite que los componentes de software y firmware sean ejecutados sobre una instalación que emplea un sistema operativo acorde con los perfiles de protección de la norma ISO/IEC 15408 (también conocida como “Common Criteria”), que hayan sido evaluados como nivel EAL 2 o superior.

FIPS 140–2 nivel 3: Incorpora mecanismos para la prevención de intrusiones, con el fin de evitar el acceso no autorizado al módulo criptográfico y de responder ante estos intentos. Tales mecanismos incluyen entre otros, el uso de circuitos de detección de tentativas de manipulación que apunten a “zeroizar ”[3] componentes cuando se intenta abrir o manipular el dispositivo. En cuanto a los mecanismos de autenticación, éstos se basan en la identidad, incrementando los requisitos establecidos para el nivel 2. En este nivel, se realiza la autenticación de la identidad de un operador y luego se verifica que se encuentre autorizado a asumir un rol determinado y a utilizar una serie de servicios. En cuanto al software y firmware, en este nivel se requiere que los sistemas operativos tengan un nivel EAL 3 o superior, con requerimientos adicionales de seguridad.

[3] La zeroización es un método de borrado o destrucción de la información almacenada en formato electrónico, basado en la alteración o eliminación de los contenidos, de manera tal que no sea posible su recuperación.

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

FIPS 140–2 nivel 4: Contiene las mayores exigencias definidas en este estándar. Los mecanismos de seguridad se plantean como un esquema de protección completa sobre el módulo criptográfico, con el objetivo de permitir la detección y respuesta ante cualquier intento de acceso físico no autorizado. Todo acceso no autorizado tiene como consecuencia la "zeroización" de los parámetros de seguridad críticos. Los módulos criptográficos que cumplen con las exigencias de este nivel son utilizados generalmente en ambientes que carecen de mecanismos adecuados de protección. Por este motivo, se prevén mecanismos de aseguramiento frente a condiciones ambientales adversas y fluctuaciones que superen los niveles operativos normales de voltaje y temperatura. En cuanto a los componentes de hardware y software, pueden ser ejecutados en un sistema que cumpla con los requerimientos del nivel 3 y tenga una evaluación EAL4 o superior.

Se recomienda la utilización de FIPS 140-2 Nivel 3 para seguridad de la Infraestructura de la Clave Pública (PKI), al ser un estándar recomendado 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.

6.3 OBLIGACIONES Y RESPONSABILIDADES DE LAS ENTIDADES DE CERTIFICACIÓN Y SERVICIOS RELACIONADOS ACREDITADAS:

En concordancia con las responsabilidades que se encuentran establecidas tanto en el modelo de acreditación emitido con Resolución Nro. 477-20-CONATEL-2008 de 08 de octubre de 2008, como en el modelo de renovación de acreditación emitido con Resolución Nro. ARCOTEL-2018-0878 de 17 de octubre de 2018, se plantean una actualización de las mismas en lo correspondiente con las Declaraciones de Prácticas de Certificación (DPC), tomando como línea base al informe presentado por la Dirección Técnica de Control de Servicios de Redes de Telecomunicaciones, en la cual realiza un análisis a las DPC de algunas entidades de certificación acreditadas, haciendo una comparación con la recomendación internacional RFC 3647.

En este contexto, se realizan inclusiones en los requisitos mínimos para la Declaración de Prácticas de Certificación que deben ser actualizadas en el modelo de acreditación y modelo de renovación antes descritos, para la prestación de los servicios relacionados. Esta declaración deberá identificarse y reconocerse en el ámbito internacional acogiendo la recomendación RFC 3647[4] o superiores de la Internet Engineering Task Force (IETF) relacionados a la materia, la cual establece los componentes principales, así como mantener 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 de historial de cambios con su fecha de actualización previa la presentación a la ARCOTEL.

[4] *https://datatracker.ietf.org/doc/html/rfc3647*

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 componentes se pueden dividir en subcomponentes, y un subcomponente puede comprender varios elementos, los cuales se desarrollan en el proyecto de resolución conforme la recomendación RFC3647, mismo que contempla los siguientes aspectos:

I. Introducción
II. Publicación y Repositorio
III. Identificación y Autenticación
IV. Requisitos operativos del ciclo de vida del certificado
V. Instalaciones, gestión y controles operativos
VI. Controles técnicos de seguridad
VII. Certificado, CRL y perfil OCSP
VIII. Auditoría de cumplimiento
IX. Otros asuntos comerciales y legales

6.4 SEGURIDAD DE LA INFORMACIÓN DE LOS CERTIFICADOS DE FIRMA ELECTRÓNICA

Los servicios de seguridad conforme el estándar ISO 7498-2[5], deben asegurar: confidencialidad; integridad; autenticación; no repudio (verificabilidad); control de acceso; y, disponibilidad. A continuación se cita estos principios:

"Confidencialidad: sólo las personas o máquinas autorizadas pueden acceder a la información transmitida a través de una red de comunicaciones o al contenido de la información guardada en un sistema informático. En algunos casos, no sólo hay que proteger el contenido de los mensajes –confidencialidad del mensaje-, sino también las identidades del emisor y del receptor –confidencialidad del tráfico de mensajes-."

"Integridad: ninguna persona no autorizada ha de poder modificar la información transmitida o almacenada. El mensaje debe llegar a su destino sin haber sufrido alteración alguna en su contenido o en el orden de la recepción de sus unidades si se compone de varios bloques."

"Autenticación: el origen de un mensaje ha de estar perfectamente identificado."

"No repudio: debe quedar constatado si un usuario envía o recibe algún mensaje. De esta manera, ni el emisor del mensaje ni el receptor del mismo pueden negar que se haya efectuado la transmisión."

"Control de acceso: sólo los usuarios autorizados debidamente identificados pueden obtener permiso de acceso a los recursos del sistema."

"Disponibilidad: el sistema no debe permitir que usuarios no autorizados dejen fuera de funcionamiento elementos de la red e impidan, así, las comunicaciones."

[5] ISO 7498-2:1989: Information processing systems -- Open Systems Interconnection -- Basic Reference Model -- Part 2: Security Architecture.

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 Ecuador, los requisitos para la validez de la firma electrónica mencionados en el artículo 15 de la Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos, están relacionados directamente con la confidencialidad, integridad, autenticación, no repudio (verificabilidad), control de acceso y disponibilidad, y para cumplirlos es necesario establecer mecanismos de seguridad que aseguren dicha validez.

Además, hay que considerar lo expuesto en el artículo 10 del Reglamento General a la Ley de comercio electrónico, firmas electrónicas y mensajes de datos vigente, donde se indica entre otros, que los principios y elementos que respaldan a la firma electrónica son las prácticas de certificación basadas en estándares internacionales o compatibles a los empleados internacionalmente y que el soporte lógico o conjunto de instrucciones para los equipos de cómputo y comunicaciones, los elementos físicos y demás componentes sean adecuados al uso de las firmas electrónicas, a las prácticas de certificación y a las condiciones de seguridad adicionales, comprendidas en los estándares señalados anteriormente; por lo que se propone los mecanismos de seguridad, para que una firma electrónica en el Ecuador sea reconocida, abordando los siguientes aspectos:

1. Mecanismos de seguridad;
2. Tipo de Seguridad;
3. Consideraciones generales respecto de las claves criptográficas (privadas y/o públicas);
4. Almacenamiento, respaldo y recuperación de las claves criptográficas de la Entidad de Certificación de Información y Servicios Relacionados Acreditada;
5. Longitud de la clave criptográfica(privadas y/o públicas);
6. Medidas de Seguridad Tecnológicas;
7. Planes de mitigación;
8. Atención virtual;
9. Entrega del producto o servicio;

A continuación se realiza una descripción de los aspectos arriba mencionados:

1. Los mecanismos de seguridad están resumidos en: algoritmos criptográficos, mecanismos de autenticación y protocolos de gestión de claves.

La Criptografía viene de los siguientes vocablos: cryptos (oculto) + grafos (escritura); y, la Criptología es igual a la Criptografía + Criptoanálisis. El proceso de los algoritmos criptográficos se diagrama en la ilustración 2:

Ilustración 2. Procesos de Algoritmos Criptográficos

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

Los objetivos de la Criptografía son la Privacidad (un intruso que escuche la comunicación no puede obtener ninguna información acerca del contenido de lo comunicado), la Autenticidad (se le da al destinatario la certeza de que la comunicación proviene del origen supuesto), y la Verificabilidad (el destinatario sabe que la comunicación es auténtica y se le da la capacidad de demostrarlo ante terceros).

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).

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 para seguridad de la Infraestructura de la Clave Pública (PKI), al ser un estándar recomendado 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.

2. Los tipos de algoritmos están enmarcados en algoritmos simétricos (las claves utilizadas para cifrar / descifrar son iguales o bien se pueden deducir fácilmente unas a partir de las otras) y algoritmos asimétricos (una de las claves es pública, mientras que la otra es secreta); ambos tipos ofrecen soluciones para los distintos servicios de seguridad.

Un algoritmo de clave pública se basa en una clave de cifrado y en una clave diferente, pero relacionada, para descifrado. Además, estos algoritmos tienen la siguiente característica importante: no es factible computacionalmente determinar la clave de descifrado solamente dado el algoritmo y la clave de cifrado. Dichos algoritmos también exhiben la característica *"cualquier clave, de las dos que se utilizan, se puede utilizar para el cifrado y la otra para el descifrado"*.

Cada sistema final en una red genera el par de claves, que se van a utilizar para cifrar los mensajes a emitir y descifrar los mensajes que se recibirán. Cada sistema publica su clave de cifrado situándola en un registro o fichero público, esta es la clave pública; mientras que la clave compañera se mantiene privada. Si A desea enviar un mensaje hacia B, cifra el mensaje utilizando la clave pública de B. Cuando B recibe el mensaje, lo descifra utilizando la clave privada de B. Ningún otro destino puede descifrar el mensaje ya que solamente B conoce la clave privada.

Con esta técnica, todos los participantes tienen acceso a las claves públicas, y las claves privadas se generan localmente por cada participante y por tanto nunca se distribuyen; mientras un sistema controle su clave privada, los mensajes que le llegan son seguros.

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

Un sistema puede cambiar su clave privada en cualquier instante de tiempo y divulga la clave pública compañera para reemplazar la clave pública obsoleta. Con esto se proporciona privacidad.

Se mencionó anteriormente que se puede utilizar cualquier clave para cifrado, utilizándose la otra para descifrado: esto habilita a que se implemente un esquema de cifrado diferente. En este caso, A prepara un mensaje para B y lo cifra utilizando la clave privada de A antes de transmitirlo. B puede descifrar el mensaje utilizando la clave pública de A. Ya que el mensaje se cifró utilizando la clave privada de A, sólo A pudo haber preparado el mensaje. Por tanto, el mensaje entero cifrado sirve como una "firma electrónica". Además, es imposible alterar el mensaje sin acceder a la clave privada de A, por lo tanto el mensaje está autenticado tanto en términos de la fuente como en términos de integridad de los datos.

La protección contra los ataques activos (falsificación de datos y transacciones) se conoce como autenticación de mensajes, que es un procedimiento que permite a las partes que se comunican verificar que los mensajes recibidos son auténticos. Los dos aspectos más importantes son verificar que el contenido del mensaje no se ha alterado y que el origen es auténtico. También hay que estar interesados en verificar que los datos son oportunos (que no han sido artificialmente retrasados y/o reemplazados) y verificar la secuencia relativa a otros mensajes que fluyen entre dos partes.

En este sentido, se plantea que estén basados 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.

Cabe mencionar que en la Recomendación X.509 se define a la Autoridad de Certificación como: *"una autoridad confiada por una o más entidades para crear y firmar digitalmente certificados de llave pública…".*[6]

3. Se tiene consideraciones generales respecto a las claves criptográficas (privadas y/o públicas) que se detallan a continuación:

    a) El par de claves deberá ser generado únicamente por la Entidad de Certificación de Información y Servicios Relacionados Acreditada utilizando infraestructura o tecnología propia o de terceros proveedores de este servicio, y deberá mantener exclusivo 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:

---

6 *"certification authority (CA): An authority trusted by one or more entities to create and digital sign public-key certificates."*
LA GUIA – MARCO DE AUTENTICACION- Reedición de la Recomendación X.509 del CCITT publicada en el Libro Azul, Fascículo VIII.8 (1988)
***Nota:** Se realizó un benchmarking con la matriz conceptual de ALADI evidenciando las recomendaciones que está utilizando el ECUADOR a través de sus Entidades de Certificación Acreditadas.*

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 clave privada sea única. Deberán utilizar como buenas prácticas aspectos como la longitud mínima, combinaciones 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.
- 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 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 con el tercero que provea la infraestructura y tecnología para la generación de las claves, de ser el caso.

4. Las Entidades de Certificación de Información y Servicios Relacionados Acreditada, deberá mantener el control exclusivo 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.

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. En la Longitud de las Claves Criptográficas (privadas y/o públicas) deberán respetarse las longitudes mínimas acorde con la Public Key Cryptographic Standards (PKCS):

   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 actividades tales como aprobar solicitudes, renovaciones, revocaciones y demás servicios de certificación, deberán mantenerse permanentemente bajo su control, 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.

6. Con la finalidad de evitar suplantaciones de identidad y/o vulneración en sus sistemas informáticos, las entidades de Certificación de Información y Servicios Relacionados Acreditadas y sus Terceros Vinculados deberán contar por lo menos con 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 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 el desarrollo de software seguros y adecuados;
   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 por lo menos una vez al año realizar un pentesting de aplicaciones y análisis de vulnerabilidades de sus sistemas por una entidad externa a la entidad especializada el cual emita un informe técnico de los resultados obtenidos y 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.

7. Para los controles de seguridad informática se tiene requisitos técnicos específicos:

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

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) **Acceso remoto:** Sólo será posible acceder a equipos configurados para este fin, y según sensibilidad del servicio, el acceso a determinadas IP previamente será autorizado, deberá utilizar túneles de conexión seguro VPN.

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 continuado 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 sobre el certificado, utilizarán técnicas de control de acceso y privilegio mínimo, de forma que los usuarios estén relacionados con las acciones que realizan y se les puede responsabilizar de sus acciones.
- Los operadores de registro, deberán firman una declaración de responsabilidad con la Entidad Certificada 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.
- Eliminación inmediata de los derechos de acceso de los usuarios que cambian de puesto de trabajo o abandonan la organización.
- Revisión periódica del nivel de acceso asignado a los usuarios.
- 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.

8. Las entidades deberán contar con planes de mitigación 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 accidentes, eventos y sus consecuencias; de acuerdo a las Políticas 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

9. 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.

   En el artículo 22 de la Ley de Comercio Electrónico, Firmas y Mensajes de Datos, sobre los requisitos del certificado de firma electrónica establece que para ser considerado válido contendrá los siguientes requisitos:

   - Identificación de la entidad de certificación de información;
   - Domicilio legal de la entidad de certificación de información;
   - Los datos del titular del certificado que permitan su ubicación e identificación;
   - El método de verificación de la firma del titular del certificado;
   - Las fechas de emisión y expiración del certificado;
   - El número único de serie que identifica el certificado;
   - La firma electrónica de la entidad de certificación de información;
   - Las limitaciones o restricciones para los usos del certificado; e,
   - Los demás señalados en esta ley y los reglamentos.

   Así mismo en el artículo 18 del Reglamento General a la Ley de Comercio Electrónico establece que es responsabilidad de la entidad certificadora de información o de la entidad de registro que actúe en su nombre, verificar la autenticidad y exactitud de todos los datos que consten en el certificado de firma electrónica. El ex CONATEL, hoy ARCOTEL podrá requerir en cualquier momento de la entidad de certificación de información, de la entidad de registro que actúe en su nombre, o del titular del certificado de firma electrónica los documentos de respaldo que confirmen la autenticidad y exactitud de los datos que contiene.

   En este sentido, las Entidades de Certificación de Información y Servicios Relacionados Acreditadas y sus Terceros Vinculados, deberán implementar los mecanismos de seguridad reforzados necesarios, incluyendo al menos dos factores de autenticación independientes y seguros como validación biométrica, prueba de vida, biometría, para verificación de la identidad de los solicitantes de certificados en todo momento, u otros mecanismos adicionales de autenticación reforzada y rigurosa con el fin de precautelar en todo momento la autenticación de los solicitantes para evitar la suplantación de identidad.

10. Para la entrega del producto y/o servicio de los certificados, los mecanismos utilizados 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 seguros adecuados. Las Entidades de Certificación de Información y Servicios Relacionados

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

Acreditada o sus Terceros Vinculados no podrán solicitar información parcial o completa, 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 titular del certificado al momento de la emisión el cambio de la misma, así como también será el responsable de su administración.

6.5 REVALIDACIÓN DEL CERTIFICADO DE FIRMA ELECTRÓNICA EMITIDA EN EL EXTRANJERO

Es importante el reconocimiento de los certificados de firmas electrónicas emitidas por Entidades de Certificación extranjeras, dado que en la Ley de Comercio Electrónico, Firmas y Mensajes de Datos en su artículo 28 establece: *"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 (...)".*

En este contexto, se propone los requisitos mínimos y el procedimiento para que los usuarios puedan revalidar los certificados de firma electrónica emitidos en el extranjero; sobre la base de procedimientos establecidos por algunas Entidades de Certificación de Información Acreditadas descritas en el informe[7] remitido por la Coordinación Técnica de Títulos Habilitantes, que se detallan en el proyecto de resolución, el cual se anexa al informe técnico.

6.6 SELLADO DE TIEMPO:

La Ley de Comercio Electrónico, Firmas y Mensajes de Datos define al sellado de tiempo de la siguiente manera: *"Anotación electrónica firmada electrónicamente y agregada a un mensaje de datos en la que consta como mínimo la fecha, la hora y la identidad de la persona que efectúa la anotación."*, adicionalmente y de acuerdo a la doctrina el sellado de tiempo es un mecanismo que permite demostrar una serie de datos de carácter electrónico que han existido y no han sido alterados desde un instante específico de tiempo, definiendo una hora y fecha específica, en que el mensaje de datos fue recibido por la entidad certificadora o el tercero registrado por la ARCOTEL; y la fecha y hora exacta en que dicho mensaje de datos fue entregado al destinatario.

Considerando que la Disposición General Segunda de la Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos, establece que este servicio debe ser acreditado técnicamente por la ARCOTEL, se proponen algunos aspectos clave

[7] Informe Nro. IT-CTHB-EC-2023-002 adjunto en el memorando Nro. ARCOTEL-CTHB-2023-1886-M de 10 de agosto de 2023.
Nota: las Entidades de Certificación Acreditadas en sus Modelos de Acreditación en la sección Responsabilidades, tiene establecido el gestionar y suscribir convenios o acuerdos de reconocimiento mutuo con Entidades Extranjeras.

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 con el sellado de tiempo, para garantizar la integridad y la autenticidad a lo largo del tiempo, como:

a) **Proceso de sellado de tiempo:** Utiliza su infraestructura para emitir sellados de tiempo digitales. Estos sellados contienen información sobre la fecha y la hora exactas en que se emitió el sellado, junto con otros datos relevantes. La Entidad de Certificación Acreditada utiliza su propia clave privada para firmar digitalmente el sellado de tiempo, lo que proporciona autenticidad y no repudio.

b) **Infraestructura de clave pública (PKI):** Suelen formar parte de una infraestructura de clave pública, que es un marco que permite la creación, distribución y gestión de certificados digitales. Los sellados de tiempo emitidos por una Entidad de Certificación Acreditada o su Tercero Vinculado están vinculados a esta infraestructura, lo que refuerza la confiabilidad y la seguridad.

c) **Uso en transacciones y documentos legales:** El sellado de tiempo por parte de una Entidad de Certificación Acreditada o su Tercero Vinculado es fundamental en situaciones donde la prueba de la cronología y la inalterabilidad de los datos es crucial. Se utiliza comúnmente en transacciones financieras, documentos legales, registros forenses y otros escenarios donde se requiere una evidencia sólida y confiable del momento en que se creó o modificó un documento digital.

d) **Estándares y protocolos:** El sellado de tiempo por parte de una Entidad de Certificación Acreditada o su Tercero Vinculado se rige por estándares y protocolos específicos, como el estándar RFC 3161 para sellados de tiempo en la red. Estos estándares aseguran la interoperabilidad y la uniformidad en la implementación del sellado de tiempo en diversos sistemas y aplicaciones.

e) **Confianza y seguridad:** La confianza en los sellos de tiempo de una Entidad de Certificación Acreditada o su Tercero Vinculado se basa en la reputación y la capacidad de dicha entidad para gestionar de manera segura su infraestructura de clave pública. Las Entidad de Certificación Acreditada deben estar sujetas a auditorías y certificaciones para garantizar la seguridad y la confiabilidad de sus servicios.

El sellado de tiempo por parte de una Entidad de Certificación Acreditada o su Tercero Vinculado desempeña un papel crucial en la garantía de la integridad y autenticidad de la información digital a lo largo del tiempo, proporcionando una evidencia sólida y confiable de la secuencia de eventos en el tiempo.

El servicio de sellado de tiempo incluye:

a) Recepción del mensaje de datos a sellar electrónicamente.

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) Los sistemas de información empleados por las Entidades de Certificación Acreditadas y su Tercero Vinculado deben garantizar como mínimo la fecha, hora y al identidad de la persona que efectúa el registro. 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.

Responsabilidad de Servicios de Sellado de Tiempo de las Entidades de Certificación de Información Acreditadas o su Tercero Vinculado serán 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 sus equipos informáticos de Sellos 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.

Se debe considerar los siguientes parámetros para el tamaño de las claves y la criptografía para el sellado de tiempo:

- 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.

Es necesario el uso de estándares y protocolos específicos para garantizar la autenticidad, integridad y confiabilidad de la marca de tiempo. Aquí se detallan los parámetros técnicos comunes utilizados en el proceso de sellado de tiempo por parte 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

una Entidad de Certificación Acreditada o su Tercero Vinculado, basados en el estándar RFC 3161[8], que se detallan en el proyecto de resolución, como:

- Tamaños de clave y criptografía.
- Declaraciones de Prácticas de Tiempo:
- Seguridades Operativas
- Protocolos de Comunicación

Estos parámetros técnicos son esenciales para asegurar la robustez y la confiabilidad del sellado de tiempo por parte de una Entidad de Certificación Acreditada o su Tercero Vinculado.

Los dispositivos de almacenamiento son los Módulos de Seguridad de Hardware (HSM, por sus siglas en inglés) son dispositivos especializados diseñados para proporcionar un entorno seguro y confiable para operaciones criptográficas. En el contexto del sellado de tiempo por parte de una Entidad de Certificación Acreditada o su Tercero Vinculado, el uso de HSM puede mejorar significativamente la seguridad, la confiabilidad y la integridad de las operaciones criptográficas asociadas con la emisión de marcas de tiempo.

A continuación se detalla algunas características que utiliza un dispositivo HSM para el sellado de tiempo:

1. Generación y Almacenamiento de Claves Criptográficas: Los HSM son utilizados para generar y almacenar de manera segura las claves criptográficas necesarias para el proceso de sellado de tiempo. Las claves privadas asociadas con la firma digital de los sellos de tiempo se almacenan dentro del HSM, protegiéndolas contra accesos no autorizados.

2. Firma Electrónica Segura: Las operaciones criptográficas, incluida la firma de los sellos de tiempo, se llevan a cabo dentro del entorno seguro del HSM. Esto reduce el riesgo de exposición de claves privadas y garantiza que las firmas sean generadas de manera segura.

3. Protección contra Ataques Físicos y Lógicos: Los HSM están diseñados para resistir tanto ataques físicos como lógicos. Esto incluye protecciones contra intentos de manipulación física del dispositivo y mecanismos para detectar y responder a actividades sospechosas.

4. Auditoría y Registro Seguro: Muchos HSM incluyen funciones de auditoría y registro que permiten rastrear y auditar las operaciones realizadas en el dispositivo. Esto es esencial para cumplir con los requisitos de seguridad y para facilitar la investigación en caso de incidentes.

[8] https://www.ietf.org/rfc/rfc3161.txt

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. Interfaz Estándar: Los HSM utilizan interfaces estándar y protocolos de seguridad para comunicarse con otros sistemas, como la Entidad de Certificación Acreditada. Esto facilita la integración del HSM en la infraestructura de la Entidad de Certificación Acreditada y garantiza la interoperabilidad.

6. Protección de la Marca de tiempo Al utilizar un HSM, se refuerza la seguridad del proceso de sellado de tiempo, protegiendo la integridad de las marcas temporales emitidas y aumentando la confianza en la evidencia temporal.

7. Conformidad con Estándares: Los HSM deben cumplir con estándares de seguridad reconocidos, como los definidos por FIPS (Federal Information Processing Standards) en los Estados Unidos o estándares equivalentes, garantizando que el dispositivo cumpla con requisitos rigurosos de seguridad.

Finalmente se proponen Disposiciones Generales y Disposiciones Transitorias para viabilizar la aplicación de la propuesta normativa.

7. CONCLUSIÓN

Sobre la base del análisis realizado se concluye que es oportuno y legítimo establecer los aspectos técnicos y procedimientos aplicables a la prestación de los servicios de certificación de información, certificados de firma electrónica, registro de datos y sellado de tiempo, así como también los deberes de los prestadores de estos servicios a través del proyecto normativo denominado *"NORMA TÉCNICA PARA LA PRESTACIÓN DE LOS SERVICIOS DE INFORMACIÓN Y SERVICIOS RELACIONADOS DE LAS ENTIDADES DE CERTIFICACIÓN ACREDITADAS Y TERCEROS VINCULADOS"*.

8. RECOMENDACIONES.

8.1 A la Coordinadora Técnica de Regulación que apruebe el presente informe como versión 2 y de considerarlo procedente se solicite a la Dirección Ejecutiva de la ARCOTEL la autorización para dar inicio al proceso de audiencias públicas de conformidad con lo dispuesto en la Resolución No. 003-03-ARCOTEL-2015 de 28 de mayo de 2015.

8.2 A la Dirección Ejecutiva que por su intermedio se solicite al Ministerio de Telecomunicaciones y de la Sociedad de la Información se deroguen los Acuerdos Ministeriales relacionados con los tipos de certificados y números identificadores de campos u OID, dado que la presente propuesta de norma ya contempla dichos aspectos, a fin de que no exista contraposición. Los Acuerdos ministeriales son los siguientes:

- Acuerdo Ministerial Nro. 181 de 15 de septiembre de 2011, a través del cual 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; y determinó los campos obligatorios de dichos tipos de certificados y números identificadores de campos u OID.

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

- Acuerdo Ministerial Nro. 006-2015 de 27 de enero de 2015, el Ministerio de Telecomunicaciones y de la Sociedad de la Información, acuerda reformar 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.

- Acuerdo Ministerial Nro. 012-2016 de 23 de mayo de 2016, con el cual 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) de los acápites 1.2.1 y 1.2.2 del artículo1, suprimiendo el tipo de certificado con la figura de Funcionario Público.

9. ANEXOS

9.1 Proyecto de Resolución
9.2 Criterio Jurídico No. ARCOTEL-CJDA-2024-0009 de 26 de enero de 2024

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:	Firma:
Ing. Fabián Marcelo Segovia Torres Analista Técnico de Regulación de Servicios y Redes de Telecomunicaciones 2	Firmado electrónicamente por: FABIAN MARCELO SEGOVIA TORRES
Ab. Alex Patricio Becerra Chingal Analista Jurídico de Regulación de Servicios y Redes de Telecomunicaciones 2	Firmado electrónicamente por: ALEX PATRICIO BECERRA CHINGAL
Revisado por:	
Ing. Jenny Paulina Zhunio Cifuentes Especialista Jefe 1	Firmado electrónicamente por: JENNY PAULINA ZHUNIO CIFUENTES

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