Expediente No. 1700203

Título Habilitante: Acreditación como una Entidad de Certificación de Información y Servicios Relacionados.

RESOLUCIÓN ARCOTEL-2018- 0902

LA AGENCIA DE REGULACIÓN Y CONTROL DE LAS TELECOMUNICACIONES

Otorga la Acreditación como Entidad de Certificación de Información y Servicios Relacionados, al Banco Central del Ecuador.

En cumplimiento de la disposición contenida en el artículo 144 numeral 29 de la Ley Orgánica de Telecomunicaciones, LOT, Disposición Final Cuarta de la LOT y artículo 37 de la Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos, que faculta a la Dirección Ejecutiva de la Agencia de Regulación y Control de las Telecomunicaciones – ARCOTEL, a dirigir el procedimiento de sustanciación y resolver sobre el otorgamiento, renovación y extinción de las acreditaciones como entidades de certificación de información y servicios relacionados, así como suscribir las correspondientes acreditaciones, en consideración a los siguientes antecedentes y fundamentos:

I ANTECEDENTES DE HECHO

Primero.- La señora Economista Verónica Artola Jarrín Gerente General del Banco Central del Ecuador, mediante comunicación dirigida a la Dirección Ejecutiva de la Agencia de Regulación y Control de las Telecomunicaciones solicitó la renovación de la Acreditación del Banco Central del Ecuador como Entidad de Certificación de Información y Servicios Relacionados adjuntando los requisitos correspondientes, establecidos en el artículo sin numerar, letra m) del Reglamento General a la Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos, reformado con Decreto Ejecutivo No. 1356 de 29 de septiembre de 2008, publicado en el Registro Oficial 440 de 06 de octubre de 2008.

Segundo.- La Unidad de Comunicación Social de la ARCOTEL procedió a publicar el 26 de julio de 2018 en la página web institucional el extracto de la solicitud para la renovación de la acreditación como Entidad de Certificación de Información y Servicios Relacionados a favor del Banco Central del Ecuador.

Como resultado de la publicación, la Unidad de Comunicación Social de la ARCOTEL, indicó que no se presentó ninguna observación al respecto.

Tercero.- Con memorando Nro. ARCOTEL-CTDS-2018-0980-M de 22 de octubre de 2018, la Dirección Técnica de Títulos Habilitantes de Servicios y Redes de Telecomunicaciones emitió el Informe unificado que contiene los informes Técnico, Económico-Financiero y Jurídico favorables Nro. CTDS-OTH-EC-2018-0237 de 22 de octubre de 2018 de la solicitud para la renovación de la acreditación como Entidad de Certificación de Información y Servicios Relacionados a favor del Banco Central del Ecuador, los cuales se pone a consideración del Director Ejecutivo de la ARCOTEL para la renovación de la acreditación como una Entidad de Certificación de Información y Servicios Relacionados en acto administrativo de acreditación que comprende el derecho para la instalación, modificación, ampliación y operación de la infraestructura requerida para tal fin.

Dirección: Av. Diego de Almagro N31-95 entre Whymper y Alpallana • **Código Postal:** 170518 / Quito - Ecuador • **Teléfono:** 593-2 294-780
www.arcotel.gob.ec

II FUNDAMENTOS DE DERECHO

Primero.- La Ley Orgánica de Telecomunicaciones – LOT, publicada en el Tercer Suplemento del Registro Oficial Nro. 439 de 18 de febrero de 2015, crea a la Agencia de Regulación y Control de las Telecomunicaciones – ARCOTEL, como una persona jurídica de derecho público, con autonomía administrativa, técnica, económica, financiera y patrimonio propio, adscrita al Ministerio rector de las Telecomunicaciones y de la Sociedad de la Información.

Segundo.- El artículo 144 de la LOT, en referencia a las competencias de la Agencia de Regulación y Control de las Telecomunicaciones ARCOTEL, establece: *"Corresponde a la Agencia de Regulación y Control de las Telecomunicaciones: (...) 29. Regular y controlar las actividades relacionadas con el comercio electrónico y firma electrónica, de conformidad con el ordenamiento jurídico vigente."*; y, la Disposición Final Cuarta, de la Ley ibídem, determina: ***"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."***. (Lo resaltado fuera del texto original)

Tercero.- la Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos, publicada en el Suplemento del Registro Oficial No. 557 de 17 de abril de 2002, regula los mensajes de datos, la firma electrónica, los servicios de certificación, la contratación electrónica y telemática, la prestación de servicios electrónicos a través de redes de información, incluido el comercio electrónico y la protección a los usuarios de estos sistemas.

La Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos, en el artículo 29, con respecto a las Entidades de Certificación de Información, determina: *"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."*; concordante con el artículo 37 de la Ley Ibídem, que establece: *"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** (...)"*. (Lo resaltado fuera del texto original)

Cuarto.- El Reglamento General a la Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos, publicado en el Registro Oficial Nro. 735 de 31 de diciembre de 2002, y reformado mediante Decreto Ejecutivo Nro. 1356 de 29 de septiembre de 2008, publicado en el Registro Oficial No. 440 de 06 de octubre de 2008, establece:

***"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. ..."*.

***"Art...-** Acreditación: La acreditación como Entidad de Certificación de Información y Servicios Relacionados, consistirá en un acto administrativo emitido por el CONATEL a través de una resolución la que será inscrita en el Registro Público Nacional de Entidades de Certificación de Información y Servicios Relacionados Acreditadas y terceros vinculados.*

El plazo de duración de la acreditación será de 10 años renovables por igual período, previa solicitud escrita presentada a la Secretaría Nacional de Telecomunicaciones con tres meses de

Dirección: Av. Diego de Almagro N31-95 entre Whymper y Alpallana • **Código Postal:** 170518 / Quito - Ecuador • **Teléfono:** 593-2 294-7800
www.arcotel.gob.ec

anticipación al vencimiento del plazo, siempre y cuando la Entidad de Certificación de Información y Servicios Relacionados Acreditada haya cumplido con sus obligaciones legales y reglamentarias, así como las que consten en la resolución de acreditación.

La acreditación como Entidad de Certificación de Información y Servicios Relacionados comprende el derecho para la instalación, modificación, ampliación y operación de la infraestructura requerida para tal fin y estará sujeta al pago de valores, los que serán fijados por el CONATEL.".

*"**Art.** ...- Requisitos para la Acreditación: El peticionario de una acreditación como Entidad de Certificación de Información y Servicios Relacionados, deberá presentar los siguientes documentos: (...)*

m) En caso de solicitud de renovación de la acreditación y de acuerdo con los procedimientos que señale el CONATEL, deberán incluirse los requisitos de carácter técnico, la certificación de cumplimiento de obligaciones por parte de la Superintendencia de Telecomunicaciones, en la que constará el detalle de imposición de sanciones, en caso de haber/as y el informe de cumplimiento de obligaciones por parte de la Secretaría Nacional de Telecomunicaciones.".

Quinto.- El ex Consejo Nacional de Telecomunicaciones CONATEL, con Resolución Nro. 477-20-CONATEL-2008 de 08 de octubre de 2018, aprobó el modelo de Acreditación como Entidad de Certificación de Información y Servicios Relacionados; con Resolución Nro. 479-20-CONATEL-2008 de 08 de octubre de 2018, publicada en el Registro Oficial Nro. 455 de 28 de octubre de 2008, expidió el *"REGLAMENTO PARA LA ORGANIZACIÓN Y FUNCIONAMIENTO DEL REGISTRO PÚBLICO NACIONAL DE ENTIDADES DE CERTIFICACIÓN DE INFORMACIÓN Y SERVICIOS RELACIONADOS ACREDITADAS Y TERCEROS VINCULADOS"*; y, con Resolución No. 480-20-CONATEL-2008 de 08 de octubre de 2018, publicada en el Registro Oficial No. 455 de 28 de octubre de 2008, fijó los valores que se deberán cancelar a la ex Secretaría Nacional de Telecomunicaciones por la Acreditación de una Entidad de Certificación de Información y Servicios Relacionados, previo a que se realice el registro respectivo, en la suma de VEINTE Y DOS MIL DÓLARES DE LOS ESTADOS UNIDOS DE AMÉRICA (USD$22,000).

Sexto.- El servicio de certificación de Información y servicios relacionados en la actualidad es prestado en régimen de competencia por empresas públicas y privadas, con lo cual, es procedente el otorgamiento de este tipo de acreditaciones.

Vistos los citados Antecedentes de Hecho y Fundamentos de Derecho, la Dirección Ejecutiva de la Agencia de Regulación y Control de las Telecomunicaciones,

RESUELVE:

ARTICULO UNO. ACREDITACIÓN.

Acreditar ante el Estado ecuatoriano al Banco Central del Ecuador legalmente representada por la señora Economista Verónica Artola Jarrín en su calidad de Gerente General, con domicilio en la Av. 10 de agosto N11-409 y Briceño de la ciudad de Quito, provincia de Pichincha, la renovación como una Entidad de Certificación de Información y Servicios Relacionados y en consecuencia, autorizarle la prestación de Servicios de Certificación de Información y Servicios Relacionados.

La acreditación como una Entidad de Certificación de Información y Servicios Relacionados comprende el derecho para la instalación, modificación, ampliación y operación de la

infraestructura requerida para tal fin y está sujeta al cumplimiento de las disposiciones contenidas en la Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos, su reglamento general de aplicación y sus reformas, la regulación, resoluciones y disposiciones que emita la ARCOTEL, así como lo señalado en este acto administrativo de Acreditación.

ARTICULO DOS. DESCRIPCIÓN DE LA INFRAESTRUCTURA, SERVICIOS Y CARACTERÍSTICAS DE OPERACIÓN.

La descripción de la infraestructura utilizada para la prestación de Servicios de Certificación de Información y Servicios Relacionados, consta en el dato técnico que se incorpora y forma parte de la presente resolución.

ARTÍCULO TRES. RESPONSABILIDADES.

La Entidad Acreditada para prestar Servicios de Certificación de Información y Servicios Relacionados, sin perjuicio de las responsabilidades contenidas en la Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos, su Reglamento General de aplicación, sus reformas y regulaciones que emita la ARCOTEL, tendrá las siguientes responsabilidades:

1. Contar con una declaración de Prácticas de Certificación, donde se especifiquen las condiciones, políticas y procedimientos aplicables a la solicitud, emisión, uso, suspensión y revocación de los certificados de firma electrónica, así como para la prestación de servicios relacionados. Esta declaración deberá contener como mínimo:

a. Datos de identificación de la Entidad de Certificación de Información y Servicios Relacionados Acreditada.
b. Condiciones de manejo de la información suministrada por los usuarios.
c. Límites de responsabilidad en la prestación de servicios de certificación de información y servicios relacionados con la firma electrónica.
d. Obligaciones de la Entidad de Certificación de Información y Servicios Relacionados Acreditada en la prestación de servicios de certificación de información y servicios relacionados con la firma electrónica.
e. Obligaciones de los usuarios y precauciones que deben observar en el manejo, uso y custodia de certificados y claves.
f. Políticas de manejo de los certificados de firma electrónica.
g. Políticas y condiciones de manejo de servicios relacionados con la firma electrónica.
h. Garantías en el cumplimiento de las obligaciones que se deriven de sus actividades.
i. Costos y tarifas de los servicios de certificación de información y servicios relacionados con la firma electrónica.

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

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

i. La seguridad de la clave privada de la Entidad de Certificación de Información y Servicios Relacionados Acreditada se vea comprometida.
ii. El sistema de seguridad de la Entidad de Certificación de Información y Servicios Relacionados Acreditada ha sido vulnerado.
iii. Se presenten fallas en el sistema de la Entidad de Certificación de Información y Servicios Relacionados Acreditada que comprometan la seguridad, disponibilidad y prestación de los servicios.

Dirección: Av. Diego de Almagro N31-95 entre Whymper y Alpallana • **Código Postal:** 170518 / Quito - Ecuador • **Teléfono:** 593-2 294-780
www.arcotel.gob.ec

b. Plan de contingencia para garantizar la continuidad y disponibilidad y de los servicios de certificación de información y servicios relacionados con la firma electrónica.
c. Procedimientos y mecanismos de seguridad para resguardo y conservación segura de la información relativa a la emisión de Certificados e información proporcionada por los usuarios.

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

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

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

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

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

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

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

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

ARTÍCULO CUATRO. OBLIGACIONES.

La Entidad Acreditada para prestar Servicios de Certificación de Información y Servicios Relacionados, sin perjuicio de las obligaciones contenidas en la Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos, su Reglamento General de aplicación reformado, y regulaciones que emita la ARCOTEL, tendrá las siguientes obligaciones:

1. Atender oportunamente las solicitudes y reclamaciones hechas por los usuarios.

2. Comprobar la veracidad, autenticidad, exactitud y validez de la información suministrada por los solicitantes del servicio, respecto de su identidad y otros datos relevantes, previo a la provisión efectiva de los servicios requeridos.

Dirección: Av. Diego de Almagro N31-95 entre Whymper y Alpallana • Código Postal: 170518 / Quito - Ecuador • Teléfono: 593-2 294-780
www.arcotel.gob.ec

3. Garantizar la protección y conservación segura de los datos personales de los usuarios, obtenidos en función de sus actividades.

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

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

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

7. Abstenerse de tomar conocimiento o acceder bajo ninguna circunstancia, a la clave privada de los usuarios titulares de Certificados de firma electrónica.

8. Publicar en su página WEB en forma permanente e ininterrumpida lo siguiente: listado de certificados emitidos, revocados y suspendidos, declaración de prácticas de certificación y políticas de seguridad, dirección de atención al público, dirección de correo electrónico de contacto, números telefónicos de contacto y el modelo de contrato de prestación de servicios de certificación de información y servicios relacionados con la firma electrónica a suscribir con los usuarios.

9. Proporcionar a los usuarios mecanismos automáticos de acceso y verificación de las listas de certificados revocados o suspendidos.

10. Poner a disposición de los solicitantes de una firma electrónica, toda la información relativa a su tramitación.

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

a. Número de solicitudes de servicio y trámite conferido a cada una de ellas.
b. Número de certificados emitidos y revocados en el mes.
c. Número de usuarios vigentes de servicios relacionados con la firma electrónica, al mes objeto del reporte.
d. Facturación total del mes.

12. Suministrar la información que requiera los entes de regulación y control, así como las entidades administrativas competentes o judiciales en relación con las Firmas Electrónicas y certificados emitidos; y, en general, sobre cualquier Mensaje de Datos que se encuentre bajo su custodia y administración.

13. Informar a la Agencia de Regulación y Control de las Telecomunicaciones, de manera inmediata, la ocurrencia de cualquier evento que comprometa la disponibilidad y la seguridad en la prestación de los servicios de certificación de información y servicios relacionados con la firma electrónica.

Dirección: Av. Diego de Almagro N31-95 entre Whymper y Alpallana • **Código Postal:** 170518 / Quito - Ecuador • **Teléfono:** 593-2 294-780
www.arcotel.gob.ec

14. Mantener actualizado en su totalidad, el registro de los certificados electrónicos revocados. Las entidades de certificación de información acreditadas, serán responsables de los perjuicios que se causen a terceros por incumplimiento de esta obligación.

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

16. Informar al usuario, dentro de las 24 horas siguientes, la suspensión del servicio o revocación de su certificado.

17. Proporcionar a los terceros que confían en los certificados emitidos por la Entidad de Certificación de Información y Servicios Relacionados Acreditada, medios razonablemente accesibles que permitan a éstos determinar mediante el certificado:

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

ARTÍCULO CINCO. COBERTURA GEOGRÁFICA O ÁREA DE OPERACIÓN.

El área de cobertura es nacional y la infraestructura para la operación, consta en el dato técnico que se anexa a la presente resolución.

ARTÍCULO SEIS. COSTOS POR RENOVACIÓN DE LA ACREDITACIÓN.

La Entidad de Certificación de Información y Servicios Relacionados Acreditada, de conformidad con la Resolución Nro. 480-20-CONATEL-2008 de 08 de octubre de 2008, canceló, previo a la suscripción del presente título habilitante, por concepto de renovación de la acreditación y autorización para prestación de servicios, la cantidad de USD 22.000,00 (VEINTE Y DOS MIL DÓLARES DE LOS ESTADOS UNIDOS DE AMERICA), de conformidad con el comprobante de pago.

ARTÍCULO SIETE. PLAZO.

El plazo de la presente renovación de acreditación es de diez (10) años, contados a partir de la fecha de inscripción del presente instrumento en el Registro Público Nacional de Entidades de Certificación de Información y Servicios Relacionados Acreditadas y terceros vinculados, prorrogable por igual período, a solicitud escrita del interesado, presentada con tres meses de anticipación al vencimiento del plazo constante en la presente Resolución y previo el cumplimiento de los requisitos técnicos, legales y económicos correspondientes.

ARTÍCULO OCHO. PROHIBICIÓN:

La Entidad de Certificación de Información y Servicios Relacionados Acreditada no podrá:

a) Ceder o transferir total o parcialmente la Acreditación, ni los derechos o deberes derivados de la misma;
b) Modificar los modelos de contratos de prestación de servicios que suscriba con sus usuarios, sin previa aprobación de la ARCOTEL; y,
c) Los cambios que vulneren derechos se consideraran como no aplicables.

Dirección: Av. Diego de Almagro N31-95 entre Whymper y Alpallana • Código Postal: 170518 / Quito - Ecuador • Teléfono: 593-2 294-780
www.arcotel.gob.ec

ARTÍCULO NUEVE. GARANTÍA.

La garantía de responsabilidad tiene por objeto precautelar y garantizar a los usuarios, la adecuada prestación de servicios de certificación de información y servicios relacionados por parte de la Entidad de Certificación de Información y Servicios Relacionados Acreditada, así como el cabal cumplimiento de las obligaciones previstas en la normativa vigente, en el presente instrumento y en el contrato de prestación de servicios con los usuarios.

La garantía se sujetará a lo establecido en el artículo innumerado denominado "Garantía de Responsabilidad" del Reglamento General a la Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos, reformado mediante Decreto Ejecutivo Nro. 1356 de 29 de septiembre de 2008 publicado en el Registro Oficial No. 440 de 06 de octubre de 2008 y a las regulaciones que emita la ARCOTEL.

El monto de la garantía a contratar por renovación, se calculará de conformidad a lo establecido en la letra b) del artículo innumerado "Garantía de Responsabilidad" del Reglamento General a la Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos, y las reformas que posteriormente existieran.

En caso de que la Entidad de Certificación de Información y Servicios Relacionados Acreditada decida terminar sus actividades en el Ecuador, la Agencia de Regulación y Control de las Telecomunicaciones ARCOTEL, luego de verificar que no se ha producido perjuicio a los usuarios del servicio, procederá a devolver la mencionada garantía a la Entidad de Certificación.

ARTÍCULO DIEZ. EXTINCIÓN O SUSPENSIÓN DE LA ACREDITACIÓN.

La presente Acreditación se extinguirá o suspenderá, sin perjuicio de las causas señaladas en la Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos y su Reglamento General de aplicación y sus reformas, por las siguientes causas:

1. Terminación del plazo para la cual fue emitida;
2. Incumplimiento de las obligaciones por parte de la Entidad de Certificación de Información y Servicios Relacionados Acreditada, previo informe motivado de la ARCOTEL;
3. Por resolución motivada de la ARCOTEL, por causas técnicas o legales debidamente comprobadas, incluyendo pero no limitadas a la presentación de información falsa o alteraciones para aparentar cumplir los requisitos exigidos, así como la prestación de servicios o realizar actividades distintas a las señaladas en la acreditación, en los casos en los que no se constituyan infracciones administrativas;
4. Cese temporal o definitivo de operaciones de la Entidad de Certificación de Información y Servicios Relacionados acreditada por cualquier causa;
5. Por no mantener vigente la garantía de responsabilidad en los términos que señala el Reglamento General a la Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos y sus reformas; y,
6. Por las causas previstas en el Código Orgánico Administrativo.

Una vez extinguida la acreditación la ARCOTEL podrá adoptar las medidas administrativas, judiciales y extrajudiciales que considere necesarias para garantizar la protección de la información de los usuarios y el ejercicio de los derechos adquiridos por estos.

Dirección: Av. Diego de Almagro N31-95 entre Whymper y Alpallana • **Código Postal:** 170518 / Quito - Ecuador • **Teléfono:** 593-2 294-780
www.arcotel.gob.ec

ARTÍCULO ONCE. ADMINISTRACIÓN DE LA ACREDITACIÓN.

La Agencia de Regulación y Control de las Telecomunicaciones ARCOTEL, dentro de sus actividades de administración de la acreditación, efectuará, entre otras, las siguientes acciones:

a) Revisar y aprobar los formatos de los contratos que la Entidad de Certificación de Información y Servicios Relacionados Acreditada suscriba con sus usuarios, así como las modificaciones que se den a los mismos;
b) Aprobar las modificaciones y ampliaciones de infraestructura o de servicios, siempre y cuando éstas no alteren el objeto de la Acreditación y no incluyan la prestación de servicios adicionales a los autorizados;
c) Realizar el procedimiento para resolver la extinción o suspensión de la Acreditación por las causales previstas en las leyes de la materia, sus reglamentos de aplicación y el presente instrumento.

Corresponde también a la Agencia de Regulación y Control de las Telecomunicaciones ARCOTEL, la supervisión y control del cumplimiento de los términos constantes en la normativa vigente y en el presente documento.

ARTICULO DOCE. DOCUMENTOS HABILITANTES.

Forman parte integrante de la presente resolución, los siguientes documentos:

a) Nombramientos del Director(a) Ejecutivo(a) de la ARCOTEL y del representante legal de la empresa (para persona jurídica);

b) Copia de la solicitud de renovación;

c) Datos Técnicos

ARTÍCULO TRECE. LEGISLACIÓN APLICABLE.

Todo lo no contemplado expresamente en esta Acreditación se sujeta a la Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos, su Reglamento General de aplicación; a la Ley Orgánica de Telecomunicaciones y su Reglamento General de aplicación, y demás normativa que expida la ARCOTEL, o la que se derive del ordenamiento jurídico.

ARTÍCULO CATORCE. ACTUALIZACIÓN NORMATIVA.

Toda reforma que se produzca a la Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos; al Reglamento General de la Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos, y en general al ordenamiento jurídico vigente en el ámbito correspondiente a la aplicación del presente título habilitante, serán de cumplimiento obligatorio para la Entidad Certificadora de Información Acreditada, debiendo dentro del plazo de 90 días de producida la modificación en el marco jurídico, realizarse la adecuación de la Acreditación, sin perjuicio de que las nuevas disposiciones sean aplicadas de manera inmediata desde la fecha de su vigencia.

Dirección: Av. Diego de Almagro N31-95 entre Whymper y Alpallana • **Código Postal:** 170518 / Quito - Ecuador • **Teléfono:** 593-2 294-780
www.arcotel.gob.ec

ARTÍCULO QUINCE. REGISTRO Y NOTIFICACIÓN.

La Agencia de Regulación y Control de las Telecomunicaciones ARCOTEL, procederá conforme a las disposiciones del Reglamento General a la Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos y del Reglamento para la Organización y Funcionamiento del Registro Público Nacional de Entidades de Certificación de Información y Servicios Relacionados Acreditadas y Terceros Vinculados, a efectuar el registro y notificación de esta Acreditación.

Dado en ....., 25 OCT 2018

Ing. Edwin Hernán Almeida Rodríguez
DIRECTOR EJECUTIVO
AGENCIA DE REGULACIÓN Y CONTROL DE LAS TELECOMUNICACIONES

ELABORADO POR:	REVISADO POR:	APROBADO POR
Dato Legal: Mgs. Carmiña Valle Dato Técnico: Ing. Xavier Páez	Ing. Carlos Altamirano	Mgs. Germán Célleri

Dirección: Av. Diego de Almagro N31-95 entre Whymper y Alpallana • **Código Postal:** 170518 / Quito - Ecuador • **Teléfono:** 593-2 294-780
www.arcotel.gob.ec

DATO TÉCNICO

DESCRIPCIÓN DE LA INFRAESTRUCTURA, SERVICIOS Y CARACTERÍSITCAS DE OPERACIÓN

DIAGRAMA ESQUEMÁTICO Y DESCRIPCIÓN TÉCNICA DETALLADA DE LA INFRAESTRUCTURA

1. OBJETIVO.

El presente documento tiene como objetivo dar a conocer una descripción técnica detallada de la infraestructura de clave pública de la Entidad de Certificación de Información del Banco Central del Ecuador (ECIBCE).

2. INTRODUCCIÓN

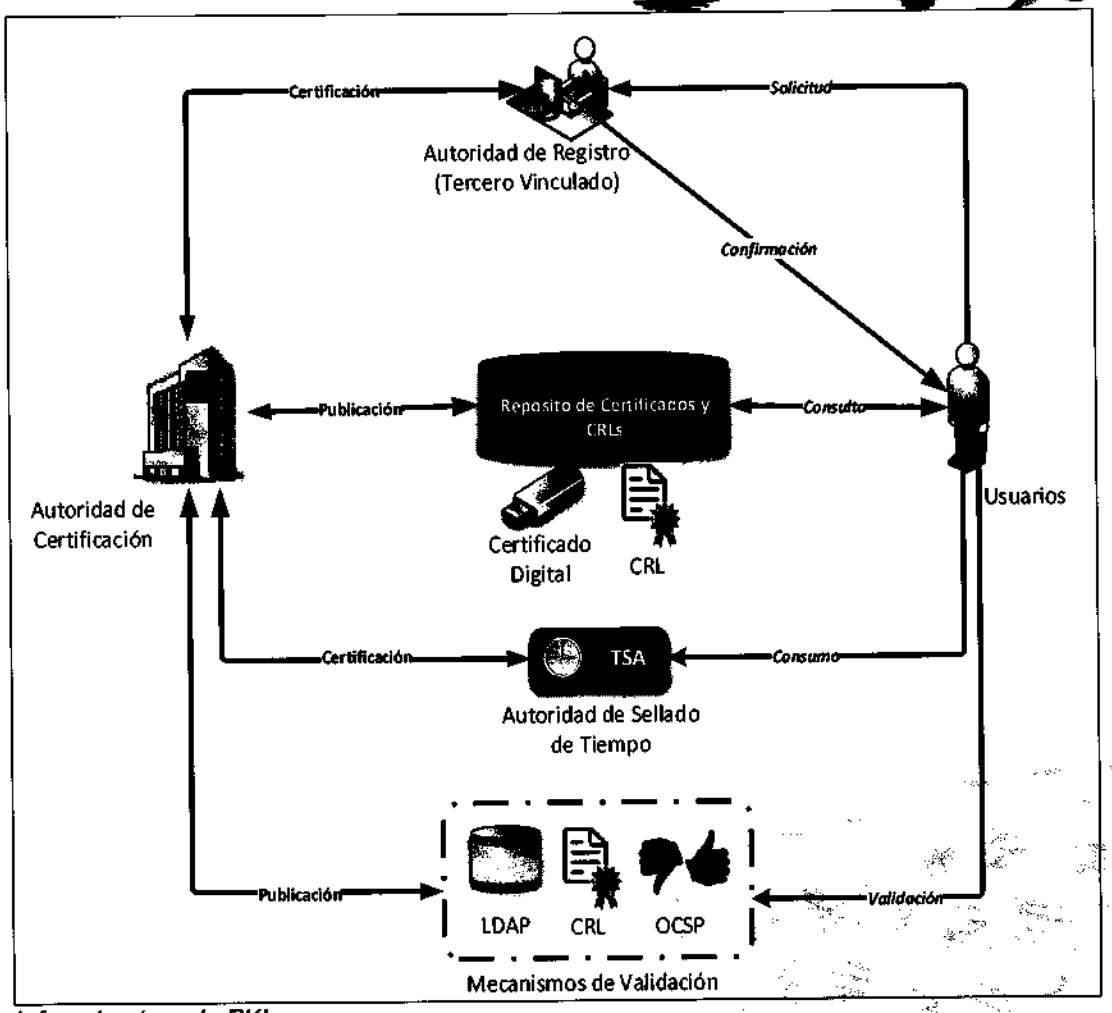
La ECIBCE como Autoridad de Certificación, (AC o CA por sus siglas en inglés Certification Authority) es una entidad de confianza, responsable de emitir y revocar los certificados digitales, utilizados en la firma electrónica, para lo cual se emplea la infraestructura de clave pública y servicios relacionados.

La ECIBCE posee una infraestructura de clave pública PKI (Public-Key-Infraestructure), que permite soportar la entrega de los servicios como Entidad de Certificación.

3. DETALLE TÉCNICO DE LA INFRAESTRUCTURA DE CLAVE PÚBLICA

Infraestructura de Clave Pública que sus siglas en ingles son PKI (Public Key Infrastructure) es una combinación de hardware y software, políticas y procedimientos de seguridad que permiten la ejecución de operaciones criptográficas garantizando la integridad, confidencialidad, no repudio y autenticidad de las transacciones electrónicas.
La tecnología PKI permite a los usuarios autenticarse frente a otros usuarios y usar la información de los certificados digitales (por ejemplo, las claves públicas de otros usuarios) para cifrar y descifrar mensajes, firmar electrónicamente información, permitir el uso en el doble factor de autenticación entre otros usos.

Dirección: Av. Diego de Almagro N31-95 entre Whymper y Alpallana • Código Postal: 170518 / Quito - Ecuador • Teléfono: 593-2 294-780
www.arcotel.gob.ec



Infraestructura de PKI

El término PKI se utiliza para referirse tanto a la Autoridad de Certificación y al resto de componentes.

La Autoridad de Certificación (o, en inglés, **CA**, Certificate Authority): es la encargada de emitir y revocar certificados. Es la entidad de confianza que da legitimidad a la relación de una clave pública con la identidad de un usuario o servicio.

La autoridad de registro (o, en inglés, **RA**, Registration Authority): es la responsable de recibir, validar, verificar y gestionar las solicitudes de emisión, revocación y renovación de certificados digitales de firma electrónica y otros servicios relacionados.

Los repositorios son las estructuras encargadas de almacenar la información relativa a la PKI. Los dos repositorios más importantes son el repositorio de certificados y el repositorio de listas de revocación de certificados – CRL, donde se incluyen todos aquellos certificados que por algún motivo han dejado de ser válidos antes de la fecha establecida dentro del mismo certificado.

La arquitectura tecnológica tiene las siguientes características generales:

Dirección: Av. Diego de Almagro N31-95 entre Whymper y Alpallana • **Código Postal:** 170518 / Quito - Ecuador • **Teléfono:** 593-2 294-780
www.arcotel.gob.ec

- Esquema de alta disponibilidad en el Centro de Cómputo principal ubicado en el Datacenter en la ciudad de Sangolquí.
- Esquema de recuperación de desastres en caso de presentarse una contingencia, considerando como sitio alterno al Centro de Cómputo ubicado en la Dirección Zonal Guayaquil en el edificio de la Corporación Financiera Nacional.
- Los componentes asociados están instalados en las áreas exclusivas y restringidas dentro de los Centros de Cómputo principal y alterno para alojar todos los componentes de la infraestructura tecnológica.
- Esquema de seguridad en capas con el fin de proteger todos los activos de información asociados a los servicios que presta la Entidad de Certificación de Información.
- Las soluciones tecnológicas para la implementación de los servicios relacionados son especializadas y requieren cumplir con estándares internacionales de seguridad y calidad que garantice la confidencialidad, integridad y disponibilidad de la información.

3.1. BCE COMO ENTIDAD DE CERTIFICACIÓN DE INFORMACIÓN

El Banco Central del Ecuador, (BCE), es la Autoridad de Certificación (AC) Raíz de su propia infraestructura de clave Pública siendo su función principal la de emitir certificados digitales, donde un certificado digital es un documento digital que asocia la identidad de un individuo (persona natural o jurídica) con su correspondiente clave pública y más atributos del estándar X.509.

En el caso específico de un certificado raíz, corresponde a un certificado que ninguna entidad de confianza superior firma digitalmente como raíz es decir posee un certificado autofirmado, y de ahí comienza la cadena de confianza. Este proceso de autofirmado hace que los campos del certificado raíz cumplan con los estándares internacionales y aplicables que garantizan la interoperabilidad.

El BCE como AC Raíz dispone de un certificado autofirmado con su propia clave privada, con el que firma los certificados digitales de las autoridades de certificación subordinada y estas emiten los certificados al usuario final, de modo que toda la jerarquía se encuentre cubierta por la confianza de la Arquitectura de la Entidad de Certificación.

La infraestructura de Claves Públicas es provista por la empresa Entrust Datacard; cuyos productos tienen certificaciones internacionales FIPS 140 y Common Criteria que garantizan que han sido desarrollados con los más exigentes estándares de seguridad.

Los certificados digitales de clave pública son generados de acuerdo al estándar X.509 que define la estructura del certificado de clave pública. El X.509 es el sector de estandarización de Telecomunicación de la Unión Internacional de Telecomunicaciones (Internacional Telecommunications Union-Telecomunications, ITU-T) y el estándar de formato de certificado de la Organization for Standarization, (ISO).

3.2. JERARQUÍA ENTIDAD DE CERTIFICACIÓN DE INFORMACIÓN DEL BANCO CENTRAL DEL ECUADOR

Autoridad de Certificación Raíz

La ECIBCE actúa como Autoridad de Certificación Raíz de la jerarquía del Banco Central del Ecuador, en la emisión de certificados para las Autoridades de Certificación Subordinadas de conformidad con los términos de la Declaración de prácticas de Certificación (DPC) vigente ***Anexo A***.

Dirección: Av. Diego de Almagro N31-95 entre Whymper y Alpallana • Código Postal: 170518 / Quito - Ecuador • Teléfono: 593-2 294-780
www.arcotel.gob.ec

Autoridad de Certificación Intermedia (Subordinada)

La ECIBCE establece Autoridades de Certificación Subordinadas para relacionar una determinada clave pública con un sujeto o entidad a través de la emisión de un certificado digital de conformidad con los términos de la DPC y de la Políticas de Certificados Natural y Jurídica (PC) vigente ***Anexo B,*** de cada tipo de certificado.

Autoridad de Registro (AR)

La ECIBCE actúa como Autoridad de Registro (AR) y, comprobará, las identidades de los solicitantes de acuerdo a lo recogido en la DPC.

La ECIBCE podrá asignar la comprobación de identidades a las oficinas del BCE que actúen como Autoridades de Registro. Las autoridades de registro comprobarán la identidad de los solicitantes de acuerdo con las normas de la DPC, la PC y el acuerdo de AR.

La ECIBCE podrá también gestionar los servicios de certificación electrónica y otros relacionados a través de terceros vinculados contractualmente y registrados en el organismo regulador.

Autoridad de Sellado de Tiempo

La Entidad de Certificación del Banco Central del Ecuador, como Autoridad de Sellado de Tiempo (TSA) es el tercero de confianza para los solicitantes, suscriptores y usuarios, quienes utilizan el servicio de Sellado de Tiempo (TS), de conformidad con los términos de la Declaración de Prácticas de Certificación de Sellado de Tiempo (DPC-ST) ***Anexo C***.

La Autoridad de sellado de tiempo del Banco Central del Ecuador provee el servicio en modalidad abierta hacia el usuario final o cerrada en una empresa a usuarios locales.

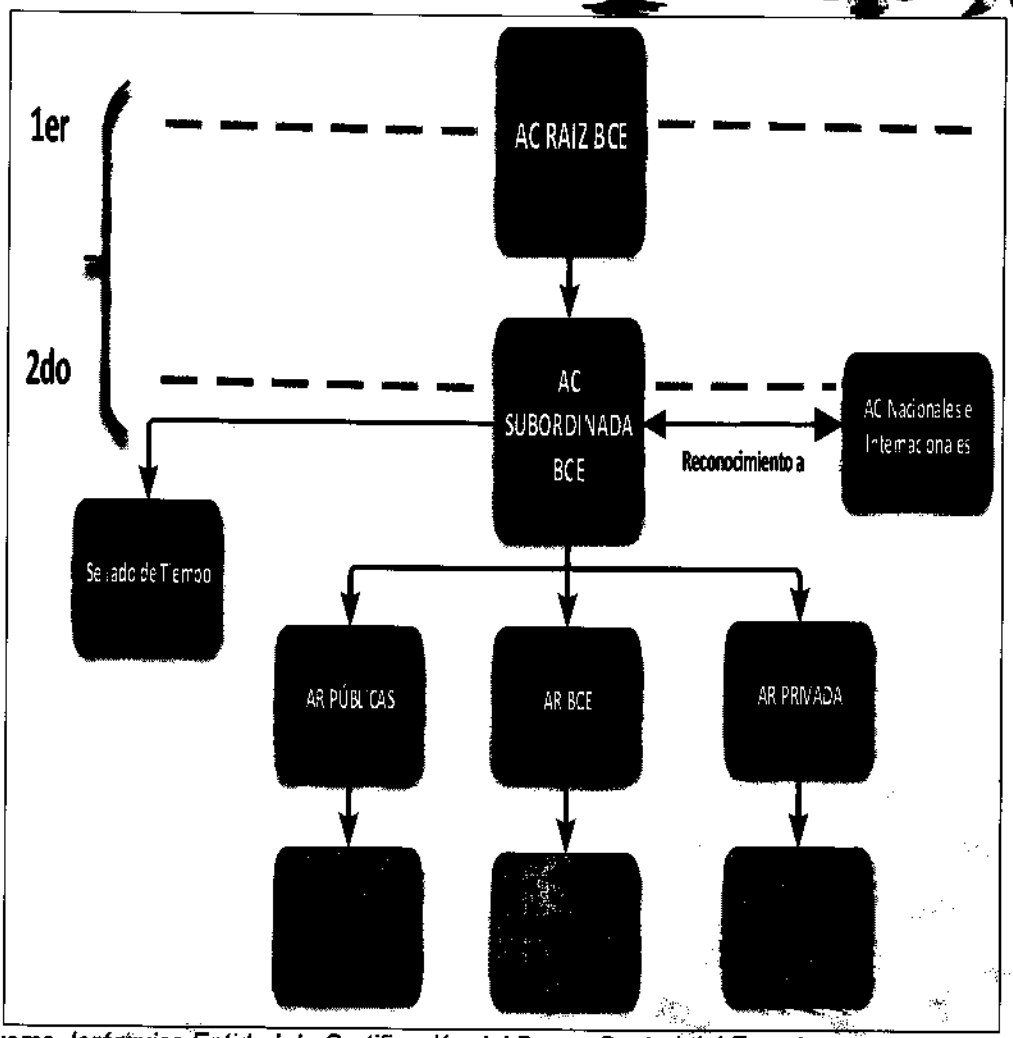
La TSA realiza la emisión de Sellos Digitales de Tiempo (TST), solicitados por los suscriptores de ese servicio; además, realiza la administración y control de la infraestructura de todos los servicios de sellado de tiempo, que se describen en la DPC-ST.

Esquema Jerárquico de la ECIBCE

La jerarquía de la ECIBCE se compone principalmente de dos niveles:

- Un primer nivel en el que se ubica la AC RAIZ de la ECIBCE que representa el punto de confianza de todo el sistema y que permite, que todas las personas naturales y jurídicas, reconozcan la eficacia de los certificados de la ECIBCE.
- Un segundo nivel, constituido por la AC Subordinada de la ECIBCE, que permite emitir los certificados digitales y sellados o estampado de tiempo.

Dirección: Av. Diego de Almagro N31-95 entre Whymper y Alpallana • **Código Postal:** 170518 / Quito - Ecuador • **Teléfono:** 593-2 294-780
www.arcotel.gob.ec



Esquema Jerárquico Entidad de Certificación del Banco Central del Ecuador

4. ADMINISTRACIÓN DE LA AC RAÍZ DEL BANCO CENTRAL DEL ECUADOR

4.1. CONTROLES DE PROCEDIMIENTO

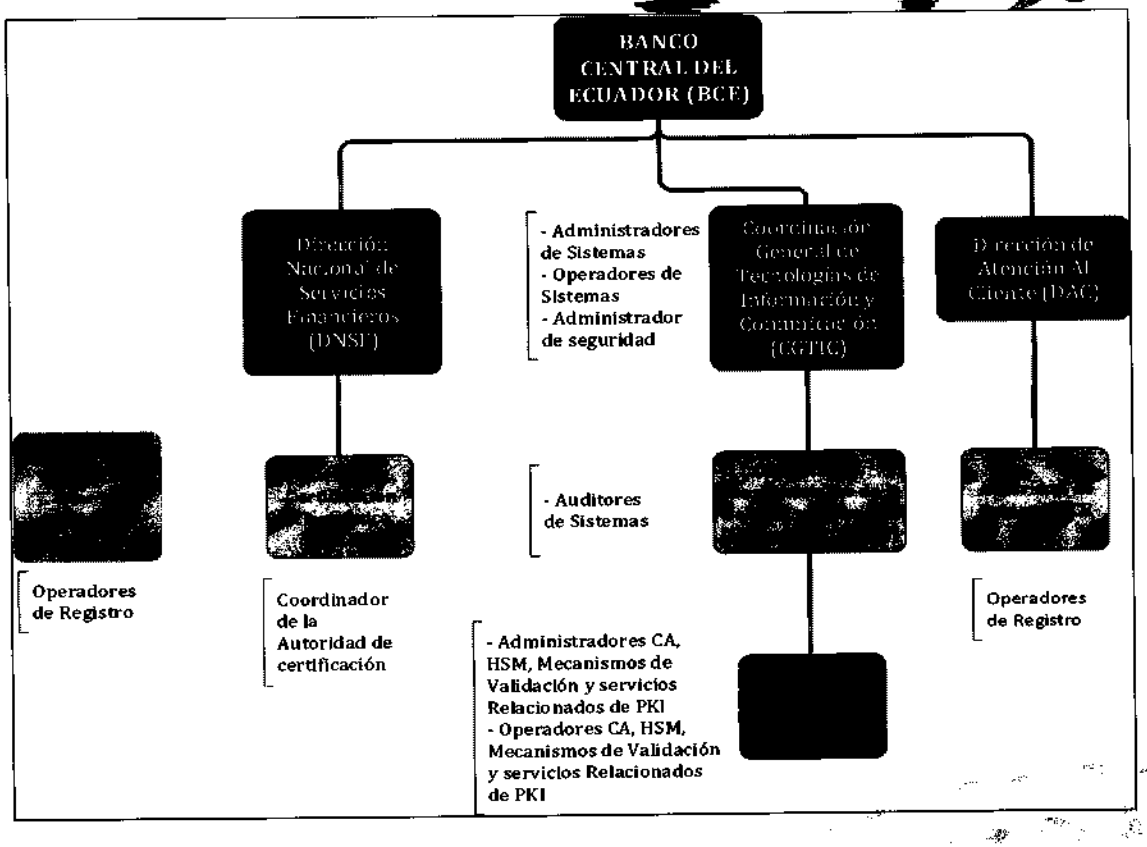
La AC Raíz del Banco Central del Ecuador procura que toda la gestión, tanto la relacionada a los procedimientos operacionales como a los de administración, se lleve a cabo de forma segura, considerando también que se puedan realizar auditorías periódicas.

Así mismo, se ha diseñado una segregación de funciones para evitar que una sola persona pueda conseguir el control total de la infraestructura.

4.2. ROLES RESPONSABLES DEL CONTROL Y GESTIÓN DE LA INFRAESTRUCTURA DE CLAVE PÚBLICA

Se distinguen los siguientes roles para la operación y gestión de la Infraestructura de clave pública:

Dirección: Av. Diego de Almagro N31-95 entre Whymper y Alpallana • Código Postal: 170518 / Quito - Ecuador • Teléfono: 593-2 294-780
www.arcotel.gob.ec



Roles para la operación y gestión de la Infraestructura de clave pública

- **Coordinador de la Autoridad de Certificación**: Tiene la responsabilidad global de administrar la implementación de las políticas y prácticas de seguridad de la AC Raíz y de la AR del Banco Central del Ecuador.

Se encargará de plantear decisiones estratégicas a la dirección de la Autoridad de Certificación y de aprobar decisiones tácticas.

Se encargará de servir de medio de comunicación entre la AC Raíz del Banco central del Ecuador y la alta dirección del Banco Central del Ecuador.

Se encargará del seguimiento y control en el desarrollo de las funciones de las funciones atribuidas a cada perfil de los descritos en este apartado y de la distribución de las tareas entre los perfiles.

Orientara al personal que conforma la AC sobre la formación a adquirir, cursos, talleres y facilitará el desarrollo de esos cursos y planes de formación.

Debe colaborar con los Auditores en todo aquellos que les sea requerido.

- **Operadores de Registro:** Se encargan exclusivamente de las funciones relacionadas con la emisión, tramitación y la revocación de certificados digitales. Estos procedimientos son realizados sobre la aplicación de la Autoridad de Registro – AR, utilizando los controles de autenticación y autorización propios del sistema. Adicionalmente, podrán

Dirección: Av. Diego de Almagro N31-95 entre Whymper y Alpallana • **Código Postal:** 170518 / Quito - Ecuador • **Teléfono:** 593-2 294-780
www.arcotel.gob.ec

suspender certificados, tras recibir la solicitud de la AC del Banco Central del Ecuador y cualquier otra actividad extraordinaria con la debida autorización.

- **Administradores de Sistemas**: Conjuntos de usuarios autorizados a realizar ciertas tareas relacionadas con la instalación, configuración y mantenimiento de la Infraestructura de Claves Públicas (PKI), pero con acceso limitado a la información relacionada con los parámetros de seguridad. Además son responsables del funcionamiento de los sistemas que componen la PKI, del hardware y del software base. La responsabilidad de este perfil incluye, entre otros, la administración de sistemas de base de datos, del repositorio de información (Mecanismos de Validación: OCSP, LDAP, CRL y Portal Web) y de los sistemas operativos. Debe velar por la prestación de servicios con el adecuado nivel de calidad y fiabilidad, en función del grado de criticidad de éstos.

- **Operadores de Sistemas:** Usuarios encargados de realizar tareas básicas del día a día como por ejemplo, ejecutar los proceso de backup y recuperación.

- **Administradores HSM (Modulo de seguridad de Hardware):** Encargados de la definición de claves de administración del HSM, de su custodia, de su configuración y puesta en marcha.

- **Operadores HSM**: Encargado de configurar el acceso al HSM por parte de las aplicaciones, de la inicialización del tokens, de asistir en las tareas de exportación e importación del material criptográfico, entre otros.

- **Administrador de seguridad:** Responsable de la definición y verificación de todos los procedimientos de seguridad. Debe cumplir y hacer cumplir las políticas de seguridad de la AC, y debe encargarse de cualquier aspecto relativo a la seguridad: física, de las aplicaciones, de red entre otros. Será el encargado de gestionar los sistemas de protección perimetral y en concreto de la gestión de las reglas de los Firewalls. Debe encargarse de la instalación, configuración y gestión de los sistemas de detección y prevención de intrusiones (IDS/IPS) y de las herramientas asociadas a éstos.

Es el responsable de resolver o hacer que se resuelvan las incidencias de seguridad producidas, de eliminar vulnerabilidades detectadas, etc. Es el responsable de la gestión y control de los sistemas de seguridad física del DPC, de los sistemas de control de acceso, de los sistemas de acondicionamiento ambiental y de alimentación eléctrica.

Debe encargarse de explicar los mecanismos de seguridad al personal que deba conocerlos, de concienciar a todo el personal de la AC y de hacer cumplir las normas y políticas de seguridad. Debe establecer los calendarios para la ejecución de análisis de vulnerabilidades, ensayos y pruebas de los planes de continuidad del servicio y auditorías de los sistemas de información. Debe colaborar con los Auditores en todo aquello que les sea requerido.

- **Auditores de Sistemas:** Autorizados a consultar archivos, trazabilidad y logs de auditoría de la Infraestructura de Clave Pública, responde a un perfil de auditor interno sin perjuicio del personal responsable de las auditorías externas.

Entre sus principales funciones:

- Constatar la existencia de toda la documentación requerida.
- Comprobar la coherencia de la documentación con los procedimientos y activos de información.
- Comprobar el seguimiento de incidencias y eventos.

Dirección: Av. Diego de Almagro N31-95 entre Whymper y Alpallana • **Código Postal:** 170518 / Quito - Ecuador • **Teléfono:** 593-2 294-780
www.arcotel.gob.ec

- Comprobar la protección de los sistemas: explotación de vulnerabilidades, logs de acceso, usuarios, etc.
- Comprobar alarmas y elementos a normativa y legislación
- Comprobar conocimiento de los procedimientos por parte del personal implicado.

4.3. IDENTIFICACIÓN Y AUTENTICACIÓN PARA CADA USUARIO AUTORIZADO

Los Administradores y Operadores del HSM se identifican y autentican en los equipos de seguridad HSM mediante dispositivos criptográficos Tokens con roles definidos a nivel de los mismos.

El resto de funcionarios de la AC del Banco Central del Ecuador se identifican mediante certificados digitales emitidos por la propia infraestructura.

La autenticación se complementa con las correspondientes autorizaciones para acceder a determinados activos de información o sistemas de la AC del Banco Central del Ecuador.

4.4. ROLES QUE REQUIEREN SEGREGACIÓN DE FUNCIONES

Entre los roles se establecen las siguientes incompatibilidades, de forma que un usuario no pueda tener dos roles marcados como "incompatibles":

- Incompatibilidad entre el rol auditor (Ej.: Auditor de Sistemas) y cualquier otro rol.
- Incompatibilidad entre los roles administrativos (Administrador de seguridad, administrador de sistema y operador de registro)
- Incompatibilidad entre los administradores y los operadores del HSM.
- Incompatibilidad entre los Administradores de seguridad y el administrador de la HSM.

4.5. CONTROLES DE PERSONAL

4.5.1. REQUISITOS RELATIVOS A LA CUALIFICACIÓN, CONOCIMIENTO Y EXPERIENCIA PROFESIONALES

Todo el personal que preste sus servicios en el ámbito de la AC del Banco Central del Ecuador posee el conocimiento, experiencia y formación suficientes, para el mejor cometido de las funciones asignadas.

4.5.2. REQUISITOS RELATIVOS A LA CUALIFICACIÓN, CONOCIMIENTO Y EXPERIENCIA PROFESIONALES

En particular, el personal relacionado con la administración y mantenimiento de la infraestructura de Claves Públicas (PKI), ha recibido la formación necesaria para asegurar la correcta realización en sus funciones. Se incluyen en la formación los siguientes aspectos:

- Entrega de una copia de la Declaración de Prácticas y Políticas de Certificación (DPC y PC).
- Operación del Software y hardware relacionado a la PKI
- Procedimientos de seguridad de la PKI (DPS)
- Procedimientos de operación y administración
- Procedimientos para la recuperación de la operación en caso de desastres (plan de contingencia).

Dirección: Av. Diego de Almagro N31-95 entre Whymper y Alpallana • Código Postal: 170518 / Quito - Ecuador • Teléfono: 593-2 294-7800
www.arcotel.gob.ec

5. **Roles y responsabilidades para Generación y Migración de llaves privadas de ECIBCE**

A más de los roles descritos para la operación y gestión de la Infraestructura de Clave Pública, la ECIBCE maneja roles para la Generación y Migración de las llaves privadas de la ECIBCE, entre los cuales se incluyen:

- Administrador de los equipos criptográficos HSM;
- Administrador técnico de aplicación de la AC;
- Encargados de particiones y Tokens;
- Custodio de materiales criptográficos;
- Coordinador de procedimiento;
- Autoridad de políticas;
- Observador independiente.

Estos roles han sido definidos para garantizar una adecuada segregación de funciones requerida para la ejecución de los procedimientos y evitar funciones incompatibles. Más de un rol podrá ser ejercido por una persona observando la segregación de funciones.

Administrador de los equipos criptográficos HSM (Delegado de la Dirección de Aseguramiento de la Calidad y Seguridad Informática)

Las responsabilidades son:

- Administrar los accesos y configurar el HSM de acuerdo a los manuales del fabricante;
- Controlar el usuario "admin" del sistema operativo del HSM y la contraseña del administrador; y,
- Entregar en sobre cerrado y lacrado, los dispositivos token y claves de protección relacionados a este rol, una vez finalizada la ejecución del procedimiento al Custodio de materiales criptográficos.

Administrador técnico de la aplicación de la AC (Delegado de la Dirección de Aseguramiento de la Calidad y Seguridad Informática)

Las responsabilidades son:

- Configurar la aplicación de la AC para realizar la integración con las HSM;
- Establecer las cuentas de usuarios de la aplicación AC; y,
- Entregar en sobre cerrado y lacrado, los dispositivos tokens y claves de protección relacionados a este rol, una vez finalizada la ejecución del procedimiento al Custodio de materiales criptográficos.

Encargados de particiones y tokens (Delegados de las áreas, en concordancia con la responsabilidad de la ejecución y del control previo y concurrente)

Las responsabilidades son:

- Controlar las Particiones y Tokens asociados a las HSM, del ambiente de producción;
- Mantener la integridad de las particiones de las HSM;
- Realizar el seguimiento de las acciones efectuadas en los dispositivos criptográficos HSM (Logs);
- Activar la conexión segura remota con los dispositivos criptográficos HSM;
- Efectuar el proceso de respaldos para precautelar la información de los dispositivos criptográficos HSM; y,

Dirección: Av. Diego de Almagro N31-95 entre Whymper y Alpallana • Código Postal: 170518 / Quito - Ecuador • Teléfonos: 593-2 294-7800
www.arcotel.gob.ec

- Entregar en sobre cerrado y lacrado, los dispositivos tokens y claves de protección relacionados a este rol, una vez finalizada la ejecución del procedimiento al Custodio de materiales criptográficos.

Custodio de materiales criptográficos (Delegado de la Dirección de Aseguramiento de la Calidad y Seguridad Informática)
Las responsabilidades son:

- Mantener un inventario preciso de los materiales del procedimiento de generación o migración de llaves de la AC incluyendo lugares de almacenaje;
- Entregar dispositivos tokens a participantes del procedimiento de generación o migración de llaves de la AC de acuerdo al rol asignado;
- Recibir de los participantes del procedimiento los dispositivos tokens en sobres sellados y lacrados posterior a la ejecución del procedimiento de migración de llaves de la AC; y,
- Asegurar que los materiales sean almacenados en forma segura posterior a la ejecución del procedimiento de generación o migración de llaves de la AC.

Coordinador del procedimiento (Director de Aseguramiento de la Calidad y Seguridad Informática)
Las responsabilidades para este procedimiento son:

- Coordinar el procedimiento de generación o migración de llaves de la AC y asegurar que las actividades definidas sean seguidas consistentemente;
- Mantener todos los registros del procedimiento de generación o migración de llaves de la AC debidamente documentados.
- Registrar cualquier desviación del procedimiento de generación o migración de llaves de la AC y registrar cualquier incidente que ocurra durante el protocolo; y,
- Aprobar cualquier desviación significativa del procedimiento de generación o migración de llaves de la AC.
- Una vez finalizado el procedimiento, notificar cualquier desviación significativa a la autoridad de políticas según corresponda.

Autoridad de políticas (Subgerente de Servicios)
Las principales responsabilidades son:

- Autorizar la ejecución del procedimiento de generación o migración de llaves de la AC; y,
- Aprobar la asignación de los roles del procedimiento de generación o migración de llaves de la AC.

Observador independiente (Delegado de la Auditoría Interna Gubernamental)
Las principales responsabilidades son:

- Atestiguar la ejecución del procedimiento de generación o migración de llaves de la AC;

El observador independiente es externo a la Gestión de Operaciones de Clave Pública responsable de la ejecución del procedimiento de generación o migración de llaves de la AC y de las operaciones actuales de la AC. El observador independiente está informado acerca de los requisitos del procedimiento de generación o migración de llaves de la AC.

Dirección: Av. Diego de Almagro N31-95 entre Whymper y Alpallana • **Código Postal:** 170518 / Quito - Ecuador • **Teléfono:** 593-2 294-780
www.arcotel.gob.ec

6. PROCESOS DE AUDITORÍA DE SEGURIDAD DE LA RAIZ DEL BANCO CENTRAL DEL ECUADOR

6.1. TIPOS DE EVENTOS GENERADOS

Se registrarán los eventos relacionados con la operación y gestión del sistema, así como los relacionados con la seguridad del mismo.

Estos registros son guardados, de manera automatizada y en los demás casos en formato papel u otros medios. Estos registros están a disposición del auditor en los casos en que sea necesario.

6.2. FRECUENCIA DE PROCESADO DE REGISTROS DE AUDITORÍA

Los registros se analizarán siguiendo procedimientos manuales y automáticos cuando sea necesario.

6.3. PERIODO DE CONSERVACIÓN DE LOS REGISTROS DE AUDITORÍA

La información generada por los registros de auditoría se mantiene en línea, los registros de auditoría se conservarán, de acuerdo a lo que establezcan las leyes y reglamentos vigentes.

6.4. PROTECCIÓN DE LOS REGISTROS DE AUDITORÍA

Los eventos registrados están protegidos mediante restricciones de acceso por roles de usuario, de forma que usuarios determinados puedan acceder estos contenidos, con su debido control.

6.5. PROCEDIMIENTOS DE RESPALDO DE LOS REGISTROS DE AUDITORÍA

Las copias de respaldo de los registros de auditoría se realizan según las políticas establecidas Banco Central del Ecuador.

6.6. ANÁLISIS DE VULNERABILIDADES

El análisis de vulnerabilidades se lleva a cabo de acuerdo a los lineamientos que establece las áreas de Seguridad y Riesgos del Banco Central del Ecuador y se ejecuta en los tiempos programados.

Dirección: Av. Diego de Almagro N31-95 entre Whymper y Alpallana • Código Postal: 170518 / Quito - Ecuador • Teléfono: 593-2 294-780
www.arcotel.gob.ec

DESCRIPCIÓN DETALLADA DE CADA SERVICIO PROPUESTO Y DE LOS RECURSOS E INFRAESTRUCTURA DISPONIBLES

7. OBJETIVO.

El presente documento tiene como objetivo dar a conocer una descripción detallada de cada servicio propuesto y de los recursos e infraestructura disponibles para su prestación, como son los mecanismos de validación: OCSP, CRL, LDAP; servicios de Sellado de Tiempo (TSA), Certificados de Servidor Seguro (SSL) y los servicios de emisión, renovación y revocación de certificados digitales para usuario final a través de la Autoridad de Registro de certificación de la Entidad de Certificación de Información del Banco Central del Ecuador (ECIBCE).

8. INTRODUCCIÓN

La ECIBCE como Autoridad de Certificación, (AC o CA por sus siglas en inglés Certification Authority) es una entidad de confianza, responsable de emitir y revocar los certificados digitales, utilizados en la firma electrónica, para lo cual se emplea la infraestructura de clave pública y servicios relacionados.

La ECIBCE posee una infraestructura de clave pública PKI (Public-Key-Infraestructure), que permite soportar la entrega de los servicios como Entidad de Certificación.

Para determinar la validez de un certificado digital de la ECIBCE, el público dispone de mecanismos de validación de certificados digitales como son servicios de OCSP, CRL, LDAP que contiene el listado de certificados revocados.

La ECIBCE presta el servicio de sellado de tiempo, ya que actúa como una Autoridad de Sellado de tiempo, a fin de entregar planes de sellado de tiempo para el público en general.

La ECIBCE provee la entrega de certificados de servidor seguro SSL para autenticar la identidad de un servidor y establecer luego un canal de transmisión seguro entre el servidor y el usuario del servicio. En general estos certificados se utilizarán para autenticar un Servidor Web mediante el protocolo SSL (o TLS).

Parte de los productos y servicios es la entrega de certificados digitales de firma electrónica a usuario final para lo cual la ECIBCE entrega servicios de emisión, renovación y revocación a través de sus Autoridades de Registro, al momento se cuenta con un Tercero Vinculado que permite brindar estos servicios con una cobertura a nivel nacional con varios puntos de emisión.

9. DESCRIPCIÓN Y ALCANCE DETALLADO DE CADA SERVICIO PROPUESTO Y DE LOS RECURSOS E INFRAESTRUCTURA DISPONIBLES PARA SU PRESTACIÓN

9.1 Situación Actual de la Infraestructura PKI del Banco Central del Ecuador

El Banco Central del Ecuador dispone de la infraestructura de clave pública que es un mecanismo que combina hardware, software, políticas y procedimientos que permiten asegurar la identidad digital de los usuarios internos como externos que consumen certificados digitales, mecanismos de validación planes de sellado de tiempo entre otros, también suministra el procedimiento que permite asegurar la identidad digital de los usuarios del sistema Nacional de Pagos que ingresan a través de la red Privada del Sistema Financiero con el uso de certificados digitales que incluyen la firma electrónica.

En el País, la firma electrónica tiene validez jurídica amparada en la ley de Comercio Electronico ***(ANEXO E)***, firmas Electrónicas y Mensajes de Datos, codificacion N0 202-67 –

Dirección: Av. Diego de Almagro N31-95 entre Whymper y Alpallana • **Código Postal:** 170518 / Quito - Ecuador • **Teléfono:** 593-2 294-780
www.arcotel.gob.ec

R.O. Sup 557 – del Miercoles 17 de abril de 2002, y su última modificación del 10 de febrero de 2014 de acuerdo a lo establecido en el Art. 13:

"Firma electrónica.- Son los datos en forma electrónica consignados en un mensaje de datos, adjuntados o lógicamente asociados al mismo, y que puedan ser utilizados para identificar al titular de la firma en relación con el mensaje de datos, e indicar que el titular de la firma aprueba y reconoce la información contenida en el mensaje de datos."

Por tanto el uso de firma electrónica se justifica plenamente debido a que en el caso de presentarse una disputa legal, puede comprobarse técnicamente que la firma corresponde a la persona que efectuó la transacción, es decir, la firma es usada como un recurso probatorio.

Adicionalmente, la firma electrónica es utilizada como una medida disuasiva, pensada también en la protección del usuario contra posibles ataques y/o fraudes electrónicos.

Por otro lado, el cifrado de datos es una técnica que permite transformar cierta información en una serie de datos ininteligibles o "datos cifrados", protegiendo la información contra usuarios no autorizados a accederla, manteniendo de esta manera la confidencialidad de la misma amparada en el Acuerdo Ministerial 166 del 25 de septiembre de 2013 y su última modificación del 15 de junio de 2016.

El siguiente cuadro resume y explica el servicio que brinda la firma electrónica y el cifrado de datos, para su diferenciación.

Cifrado de Datos	Confidencialidad	Esquema Gubernamental de Seguridad de la Información - EGSI ***(ANEXO F)***
Firma Electrónica	• Autenticidad • Integridad • No repudio o Aceptación	Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos

10. DESCRIPCIÓN DETALLADO DEL SERVICIO PROPUESTO COMO ENTIDAD DE CERTIFICACIÓN

Las organizaciones actuales se orientan a la conservación y respaldo de la información que manejan a través de modelos de seguridad que permite brindar sus servicios de forma confiable con el resguardo de toda información sensible considerando mecanismos de identificación, autenticación, autorización, integridad y confidencialidad, en el Ecuador la Ley de Comercio Electrónico, Firmas y Mensajes de Datos, regula los mensajes de datos, la firma electrónica, los servicios electrónicos, a través de redes de información, incluido el comercio electrónico y la protección de los usuarios de estos sistemas.

De esta manera la Entidad de Certificación de Información del Banco Central a través del uso de su Infraestructura de Clave Pública – PKI (Public Key Infraestructure) permite crear las identidades digitales y la confianza que se necesita para los procesos de identificación y autenticación así como la administración de las claves públicas y privadas de los usuarios. El manejo de los certificados digitales en combinación con las claves públicas y privadas, permite la identificación precisa de los participantes mediante la validación de su identidad, y el acceso a la información requerida sólo al personal autorizado (control de acceso), asegurando la confidencialidad e integridad de los datos gracias a las técnicas de criptográficas o de cifrado de datos.

El papel primario de la Infraestructura PKI es establecer identidades digitales confiables entre sus participantes, es decir, el Banco central del Ecuador actúa como el tercero confiable entre las instituciones participantes, ofreciendo un nivel de credibilidad razonable en el proceso que

Dirección: Av. Diego de Almagro N31-95 entre Whymper y Alpallana • Código Postal: 170518 / Quito - Ecuador • Teléfono: 593-2 294-780
www.arcotel.gob.ec

usa para emitir los certificados digitales en conjunción con las claves públicas y privadas, demostrando que la identidad que crea y los mecanismos de identificación que utiliza son veraces y legalmente aceptados.

La infraestructura PKI requiere de directivas o políticas de seguridad, de software y hardware especializados que permitan la seguridad y fácil administración, de administradores que soporten todo la infraestructura y atiendan los requerimientos de los usuarios.

Los componentes tecnológicos de la infraestructura PKI del Banco Central del Ecuador son los siguientes:

Autoridad de Certificación (AC)	Entrust Authority Security Manager	Red Hat Enterprise Linux 5.4
Autoridad de Certificación Subordinada	Entrust Authority Security Manager	Microsoft Windows Server 2008 R2
Repositorio de Certificados Digitales (LDAP RAIZ)	Open Ldap	Red Hat Enterprise Linux 6.0
Repositorio de Certificados Digitales (LDAP Subordinado)	Open Ldap	Red Hat Enterprise Linux 6.0
Administration Services	Entrust Authority™ Administration	Microsoft Windows Server 2008 R2
Lista de Certificados Revocados	Apache	Red Hat Enterprise Linux 6
Protocolo de comprobación del Estado de un Certificado En línea (OCSP)	**OCSP-EJBCA**	Red Hat Enterprise Linux 5.5
Protocolo de comprobación del Estado de un Certificado En línea (OCSP)	**KeyOne Validation Authority**	Microsoft Windows Server 2012 R2 Standar
Contenedor Certificado Roaming	Entrust Authority™ Roaming Server	Microsoft Windows Enterprise 2008
Contenedor Certificado Archivo	Entrust Authority™ Digital Identity Manager	Microsoft Windows Server 2008 R2 Enterprise
Contenedor Certificado Token	Api Generación Certificados en contenedor Token	Solaris 10
Sellado de Tiempo	Ascertia	Microsoft Windows Server 2012 R2 Standar

Adicionalmente, y con el fin de garantizar la disponibilidad de los servicios asociados a la infraestructura PKI, el Banco Central del Ecuador dispone de una arquitectura de alta disponibilidad y desarrolló un plan de contingencia, considerando como sitio alterno a la Dirección Zonal Guayaquil.

Dirección: Av. Diego de Almagro N31-95 entre Whymper y Alpallana • Código Postal: 170518 / Quito - Ecuador • Teléfono: 593-2 294-780
www.arcotel.gob.ec

11. MECANISMOS DE VALIDACIÓN: CRL, OCSP, LDAP

La ECIBCE, dispone de mecanismos de validación a través de la lista de certificados revocados con el fin de mantener la confiabilidad de los certificados emitidos por la Entidad de Certificación, los mecanismos son:

- Servicio de Listas de Certificados Revocados (CRL)
- Servicio de Consulta en Línea de Certificados Digitales (OCSP)
- Servicio de Repositorio de Certificados Digitales (LDAP)

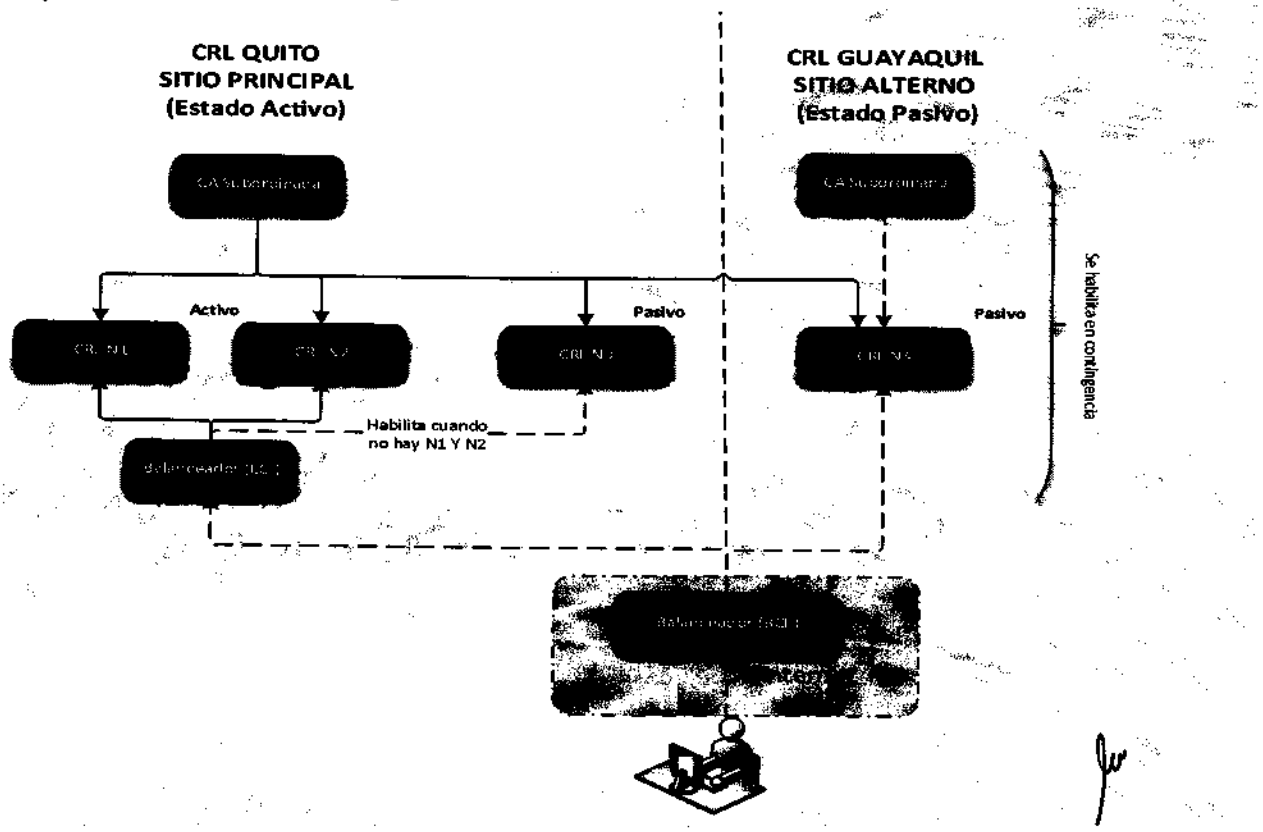
a. **Servicio de Listas de Certificados Revocados (CRL)**

La lista de certificados revocados, conocida por sus siglas en ingles CRL (Certificate Revocation List), es una lista de certificados que han sido revocados donde se reflejan los números de serie de los mismos, no válidos y en los que no debe confiar ningún usuario de un sistema.

La CRL tiene un periodo de vigencia de 25 horas para los certificados de usuario y la ARL (Authority Revocation List) un periodo de 9 meses para los certificados de Autoridad de Certificación.

La publicación de las CRLs está disponible en la página web de la Entidad de Certificación 24 horas, 365 días con un esquema de alta disponibilidad, ya que es un servicio crítico que consumen los usuarios de forma permanente.

Arquitectura CRL de la ECIBCE



Arquitectura CRL de la ECIBCE

Dirección: Av. Diego de Almagro N31-95 entre Whymper y Alpallana • Código Postal: 170518 / Quito - Ecuador • Teléfono: 593-2 294-780
www.arcotel.gob.ec

El servicio de CRL entregado por el Banco Central de Ecuador de acuerdo al gráfico antes señalado esta compuesto en el sitio principal Quito por dos nodos activos y balanceados, y un nodo pasivo esta listo para entrar en operación en caso de no disponibilidad de los nodos activos.

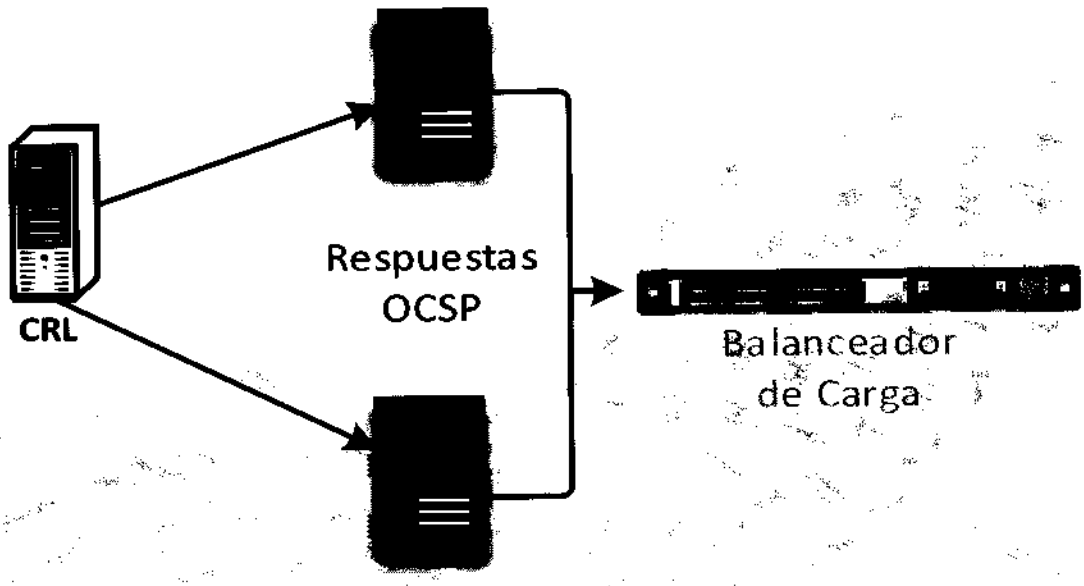
Como contingencia en sitio alterno Guayaquil se dispone de un nodo pasivo en caso de existir eventos de fuerza mayor que no permitan prestar el servicio desde el sitio principal Quito.

Estos servicios están sobre infraestructura de alta gama en servidores de tipo cuchuilla (blades) de altas prestaciones y en modo cluster, a fin de garantizar los servicios de manera continua y permanente.

Servicio Consulta en Línea de Certificados Digitales (OCSP)

Online Certificate Status Protocol (OCSP) es un método para determinar el estado de vigencia de un certificado digital X.509 y permite determinar si el certificado se encuentra revocado o no. Este protocolo se describe en el RFC 2560 y está en el registro de estándares de Internet.

Los mensajes OCSP se codifican en ASN.1 y habitualmente se transmiten sobre el protocolo HTTP. La naturaleza de las peticiones y respuestas de OCSP hace que a los servidores OCSP se les conozca como "OCSP responders".

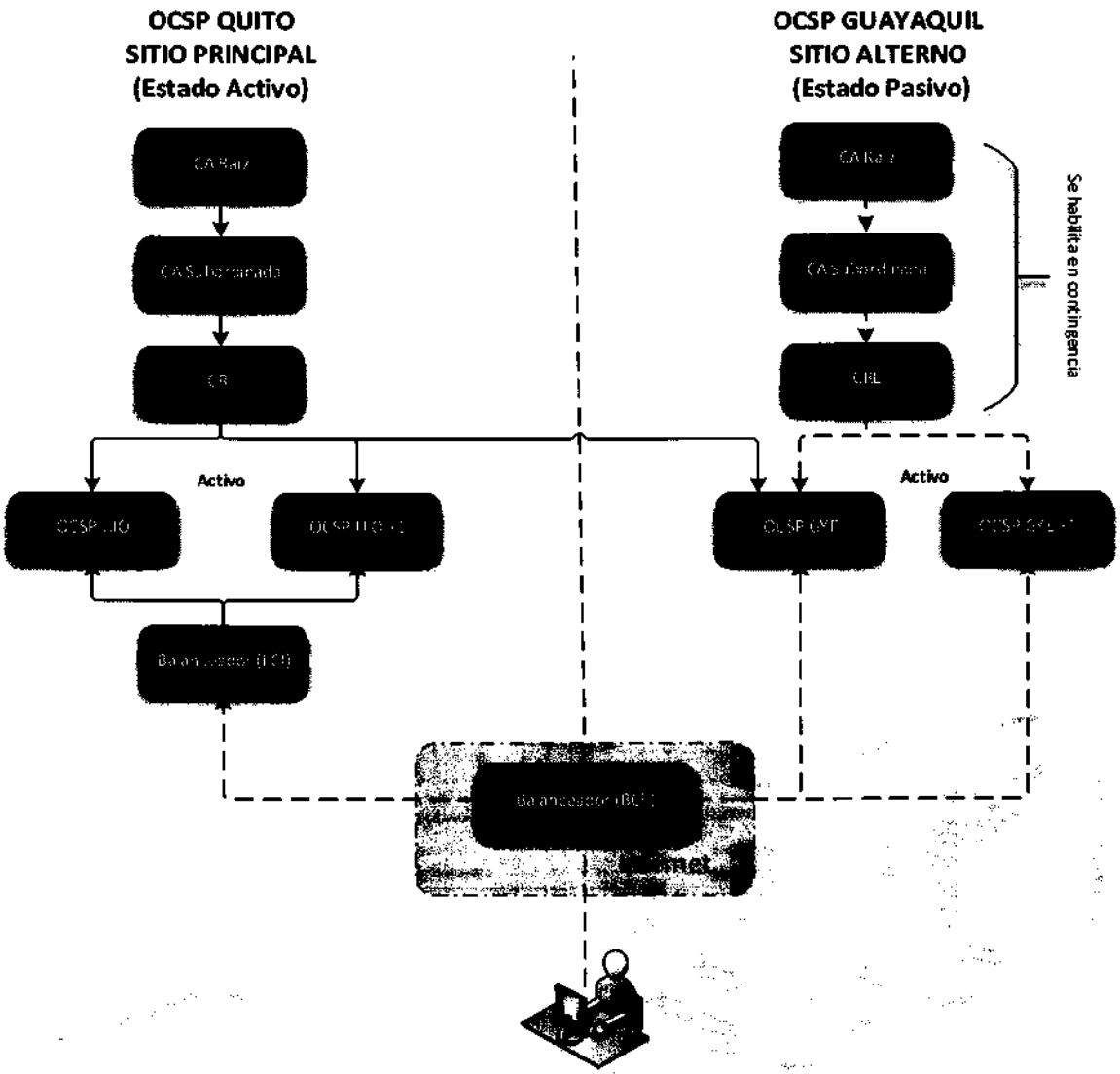


Mecanismo de Validación OCSP

El OCSP es un componente complementario en la Infraestructura de Clave Pública que en sus siglas en ingles PKI significa (Public Key Infrastructure).

Dirección: Av. Diego de Almagro N31-95 entre Whymper y Alpallana • **Código Postal:** 170518 / Quito - Ecuador • **Teléfono:** 593-2 294-780
www.arcotel.gob.ec

Arquitectura OCSP de la ECIBCE



Arquitectura OCSP de la ECIBCE

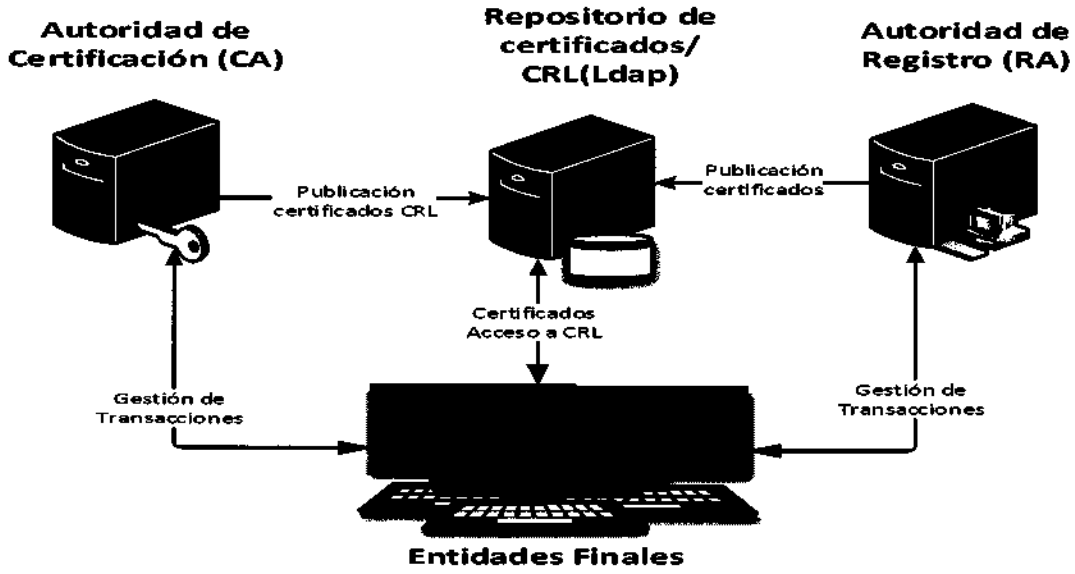
El servicio de OCSP entregado por el Banco Central de Ecuador de acuerdo al gráfico antes señalado esta compuesto en el sitio principal Quito por tres nodos activos y balanceados, y en sitio alterno Guayaquil dos nodos adicionales en estado activo con la finalidad de soportar la alta demanda de peticiones de validación de certificados digitales.

Estos servicios están sobre infraestructura de alta gama en servidores de tipo cuchuilla (blades) de altas prestaciones y en modo cluster, a fin de garantizar los servicios de manera continua y permanente.

Servicio Repositorio de Certificados Digitales (LDAP)

LDAP son las siglas de **L**ightweight **D**irectory **A**ccess **P**rotocol (en español Protocolo Ligero/Simplificado de Acceso a Directorios) que hacen referencia a un protocolo a nivel de

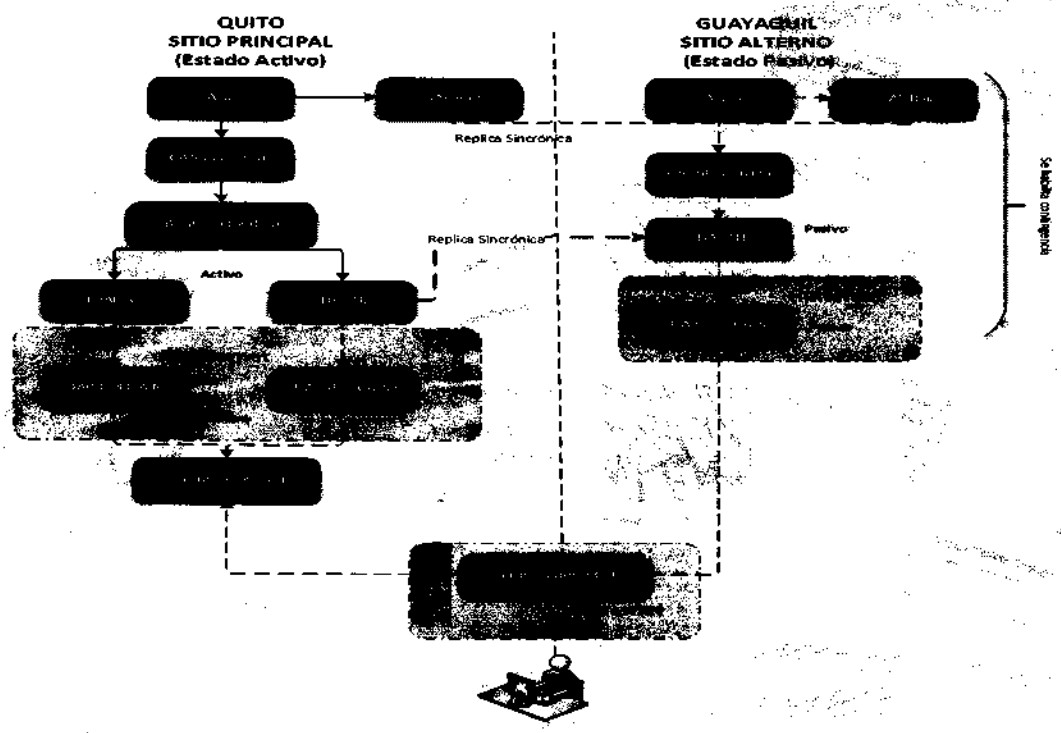
aplicación que permite el acceso a un servicio de directorio ordenado y distribuido para buscar diversa información en un entorno de red.



Estructura Ldap

Las CRL son parte del directorio LDAP, y es un componente esencial en la Infraestructura de Clave Pública que en sus siglas en ingles PKI significa (Public Key Infrastructure).

Arquitectura LDAP de la ECIBCE



Arquitectura LDAP ECIBCE

Dirección: Av. Diego de Almagro N31-95 entre Whymper y Alpallana • **Código Postal:** 170518 / Quito - Ecuador • **Teléfono:** 593-2 294-780
www.arcotel.gob.ec

El servicio de repositorio de certificados digitales LDAP entregado por el Banco Central de Ecuador de acuerdo al gráfico antes señalado está compuesto en el sitio principal Quito por dos nodos activos y balanceados. De forma similar se dispone de una replicación de los repositorios LDAPS expuestos a Internet para las consultas de los clientes.

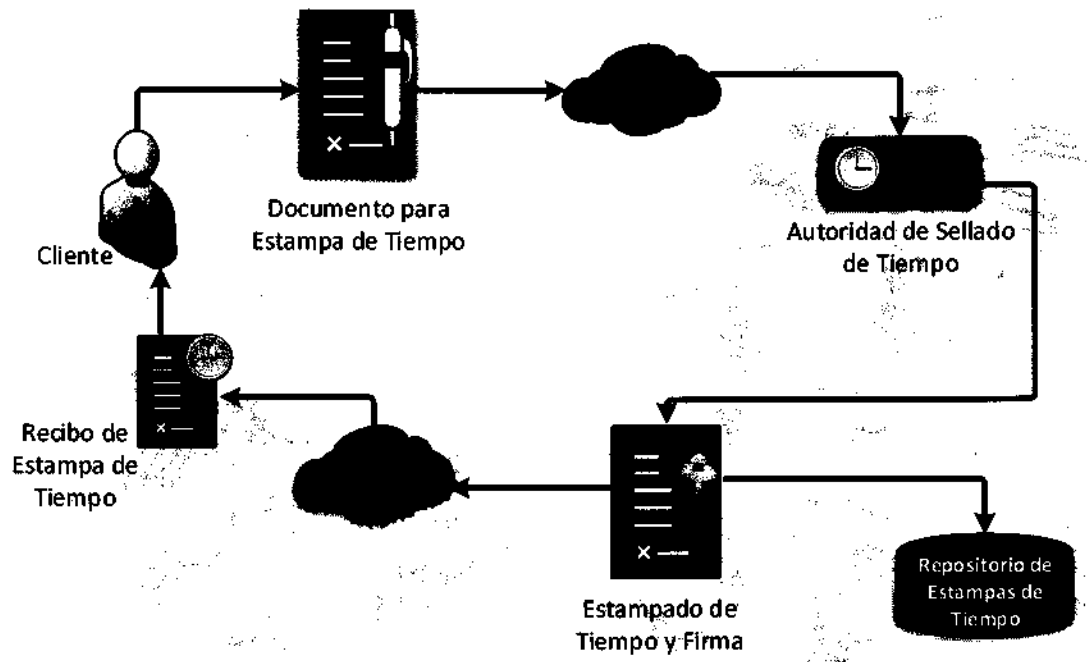
Como contingencia en sitio alterno Guayaquil se dispone de un nodo pasivo en caso de existir eventos de fuerza mayor que no permitan prestar el servicio desde el sitio principal Quito.

Estos servicios están sobre infraestructura de alta gama en servidores de tipo cuchuilla (blades) de altas prestaciones y en modo cluster, a fin de garantizar los servicios de manera continua y permanente.

12. SELLADO DE TIEMPO (TSA – Time Stamp Authority)

Es un servicio que permite asegurar el momento en que un documento electrónico fue creado, es emplear una tercera parte de confianza, comúnmente llamada una autoridad de sellado de tiempo (TSA), para mayor información refiérase al ***ANEXO C Declaración de Prácticas de Certificación de Sellado de Tiempo (DPC-ST).***
Dentro del proceso de envío y recepción del documento firmado digitalmente con su respectiva fecha y hora el Banco Central actúa como una tercera parte de confianza, comúnmente llamada una autoridad de sellado de tiempo (TSA) para vincular una hora a la firma digital en el momento en que la firma fue creada o cerca de la creación de la misma.

La solución del servicio de sellado de tiempo incluye una aplicación que le permitirá al usuario sellar el documento (hora y fecha) generando una mayor seguridad, garantía y validez al mismo.



Sellado de Tiempo

El BCE como Autoridad de Sellado de Tiempo (TSA) cuenta con las siguientes características:

- Utiliza una fuente fiable de tiempo (INOCAR).
- Incluye un valor de tiempo de confianza para cada sellado de tiempo.
- Genera un número único para cada sellado de tiempo.

- Para producir un sellado de tiempo es necesario recibir una solicitud válida del solicitante.
- Debe ser posible el estampado de tiempo con firmas SHA1y SHA256.

Sistema de Tarificación de Servicios de Sellado de Tiempo

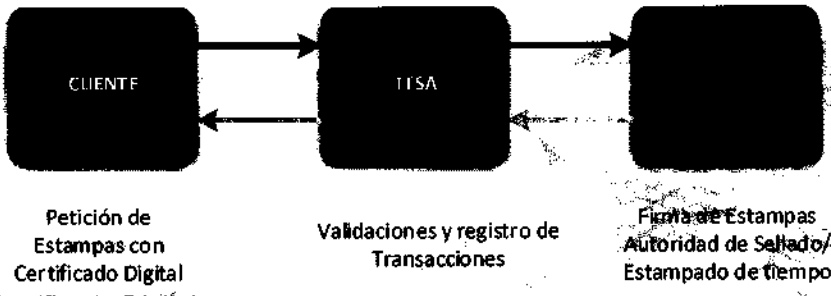
El propósito general de TTSA es de servir de intermediario entre un cliente final, que utiliza servicios de sellado de tiempo, y un proveedor de dichos servicios. Al proveedor de los servicios de sellado de tiempo se llama Autoridad de estampado o sellado de tiempo "TSA".

Al ser un intermediario, el TTSA permite tener control sobre todas las peticiones que se envían a la TSA, de manera que puede proveer varios servicios adicionales. Esto implica que se pueden hacer validaciones adicionales sobre quién envía las peticiones, y llevar un registro de todas las estampas firmadas por la TSA.

Existen dos mecanismos de conexión para el consumo de sellos o estampas de tiempo:

(1er Mecanismo) mediante Certificado Digital

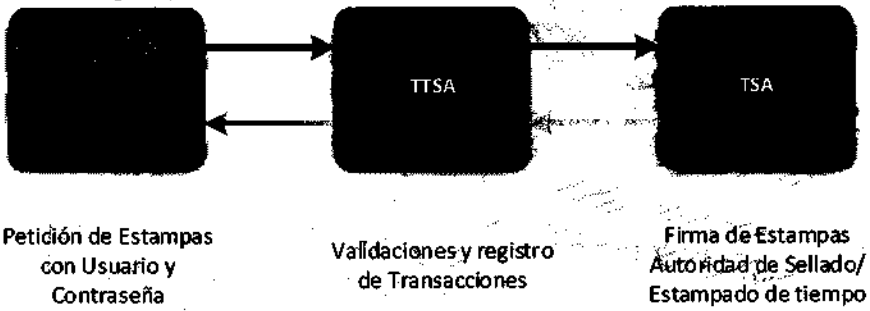
La utilización de este mecanismo de estampas de tiempo en su autenticación se requiere de librerías con las que cuenta la Entidad de Certificación del Banco Central del Ecuador, y un **certificado digital en formato p12 o pfx** que se utiliza para **autenticarse** y consumir el servicio desde el equipo o servidor que este destinado para el efecto. (Se entrega un ejemplo (API genérico JAVA o .NET) de generación de TSQ - petición de sellos de tiempo y se obtiene un TSR - respuesta a petición de sellos de tiempo)



TSA con Certificado Digital

(2do Mecanismo) mediante Usuario y Contraseña

A diferencia del anterior mecanismo el **cliente** se autentica a través de **usuario y contraseña** sin un certificado digital para la autenticación, a través del portal Web www.eci.bce.ec.



TSA con Usuario y Contraseña

- JsignPDF
- Adobe standar o profesional
- Código disponible para Java y .NET (BounceCasttle, Itext, etc)

Clientes actuales y potenciales:

Los clientes que consumen este servicio son generalmente corporaciones e instituciones públicas que por la criticidad y naturaleza de sus negocios exigen contar con certificación del tiempo que les permita asegurar el momento exacto de las transacciones realizadas, entre algunas se menciona:

- *CONECEL,*
- *OTECEL,*
- *ETAPA,*
- *SERCOP,*
- *CNT,*
- *REGISTRO CIVIL, entre otros.*

Entre los usos se puede mencionar algunos como por ejemplo: seguridad en transacciones electrónicas, emisión de pólizas electrónicas, procesos de recepción de balances por parte de las empresas.

Condiciones del Servicio

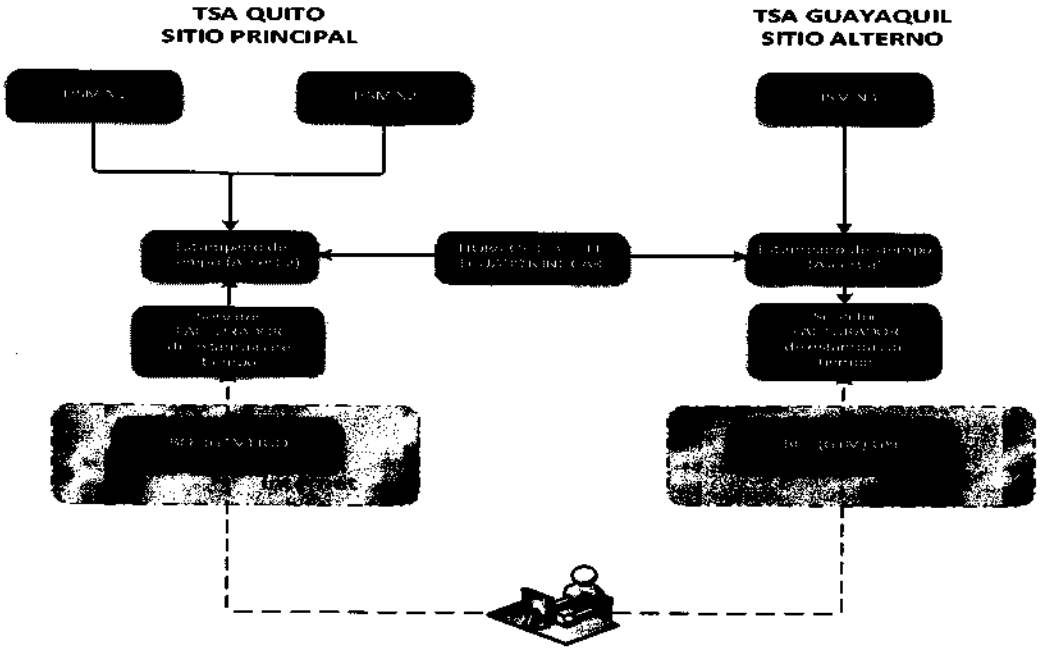
1 La solicitud del servicio de sellado de tiempo se realiza en formulario pre-establecido enviado por la Entidad de Certificación.
2 Una vez recibida la solicitud con los requisitos ésta será aprobada y se deberá proceder al pago.
3 El BCE enviará mediante correo electrónico a la persona de contacto, un usuario y clave para acceder a un portal que le permita monitorear el consumo de los sellos de tiempo.
4 El BCE y el cliente procederán a la firma del contrato, de prestación de servicios, una copia será entregado al cliente.

Arquitectura TSA de la ECIBCE

La arquitectura del Servicio de Estampado de Tiempo de la Entidad de Certificación de Información del Banco Central del Ecuador – ECIBCE, se sustenta bajo los conceptos de la seguridad de la información que consisten en la preservación de la confidencialidad, integridad y disponibilidad, así como de los sistemas implicados en su tratamiento, términos definidos normas ISO de la siguiente manera:

a. Confidencialidad: Se garantiza que la información sea accesible sólo a aquellas personas autorizadas a tener acceso a ella.
b. Integridad: Se salvaguarda la exactitud y totalidad de la información y los métodos de procesamiento.
c. Disponibilidad: Se garantiza que los usuarios autorizados tengan acceso a la información y a los recursos relacionados con ella siempre que se requiera.

Dirección: Av. Diego de Almagro N31-95 entre Whymper y Alpallana • **Código Postal:** 170518 / Quito - Ecuador • **Teléfono:** 593-2 294-780
www.arcotel.gob.ec



Arquitectura TSA de la ECIBCE

El servicio de sellado de tiempo entregado por el Banco Central de Ecuador de acuerdo al gráfico antes señalado esta compuesto en el sitio principal Quito por un nodo activo y en sitio alterno Guayaquil un segundo nodo activo balanceados geograficamente.

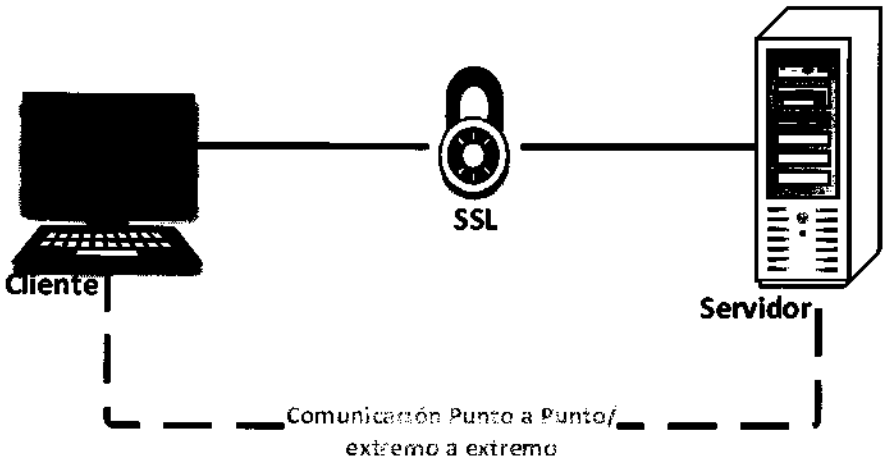
Estos servicios estan sobre infraestructura de alta gama en servidores de tipo cuchuilla (blades) de altas prestaciones y en modo cluster, a fin de garantizar los servicios de manera continua y permanente.

13. CERTIFICADOS DE SERVIDOR SEGURO (SSL)

Los Certificados de Servidor Web son certificados expedidos a entidades públicas o privadas para servidores seguros o web. La finalidad del certificado es autenticar de forma segura el servidor en la red y permitir a los usuarios crear una conexión segura mediante protocolos criptográficos estándar, como SSL o TLS. Toda la información contenida en el certificado para servidor seguro es suministrada a la entidad que actúa como Autoridad de Registro por el propio suscriptor bajo su entera responsabilidad.

La información enviada desde un usuario hacia el Servidor Seguro viaja encriptado, por lo que de ser interceptada es imposible de descifrar. Además la información se marca digitalmente, lo que permite verificar si fue alterada en el trayecto que viaja la información.

Dirección: Av. Diego de Almagro N31-95 entre Whymper y Alpallana • **Código Postal:** 170518 / Quito - Ecuador • **Teléfono:** 593-2 294-780
www.arcotel.gob.ec



Certificado SSL

Usos del Certificado

Los Certificados de Servidor seguro pueden ser utilizados para autenticar la identidad de un servidor, y establecer luego un canal de transmisión seguro entre el servidor y el usuario del servicio. En general estos certificados se utilizarán para autenticar un Servidor Web mediante el protocolo SSL (o TLS).

El titular sólo puede utilizar la clave privada y el certificado de acuerdo con lo establecido en los campos "Uso de clave" y "Uso Mejorado de claves" del certificado, los usos no autorizados así como mayor detalle de las limitaciones de estos certificados se definió en la DPC y PC.

Clientes actuales y potenciales:

Los certificados SSL que emite la Entidad de Certificación de Información del Banco Central del Ecuador están definidos exclusivamente para garantizar la seguridad y confiabilidad de la comunicación entre las aplicaciones desarrolladas por el Banco Central del Ecuador con las instituciones participantes en el Sistema Nacional de Pagos y para identificar un dominio para aplicaciones internas al Banco Central, entre los aplicativos del BCE que consumen el servicio tenemos:

- *Sistema Nacional de Pagos,*
- *Dominios Internos BCE*

Condiciones del Servicio

1 La solicitud del servicio para la obtención del certificado SSL se realiza en un formulario pre-establecido enviado por la Entidad de Certificación.
2 Una vez enviada la solicitud con los requisitos ésta será aprobada y se deberá proceder al pago.
3 La ECIBCE enviará mediante correo electrónico a la persona de contacto (cliente), los códigos habilitantes (Reference Number) para la generación de la clave privada (.key) y el archivo de petición de firma CSR (request) con una longitud de 2048 bits y SHA256.
4 La ECIBCE efectúa la verificación de la petición (Request) y procede a la emisión del certificado SSL (clave pública .CER).
5 El BCE y el cliente procederán a la firma del contrato, de prestación de servicios, una copia será entregado al cliente.

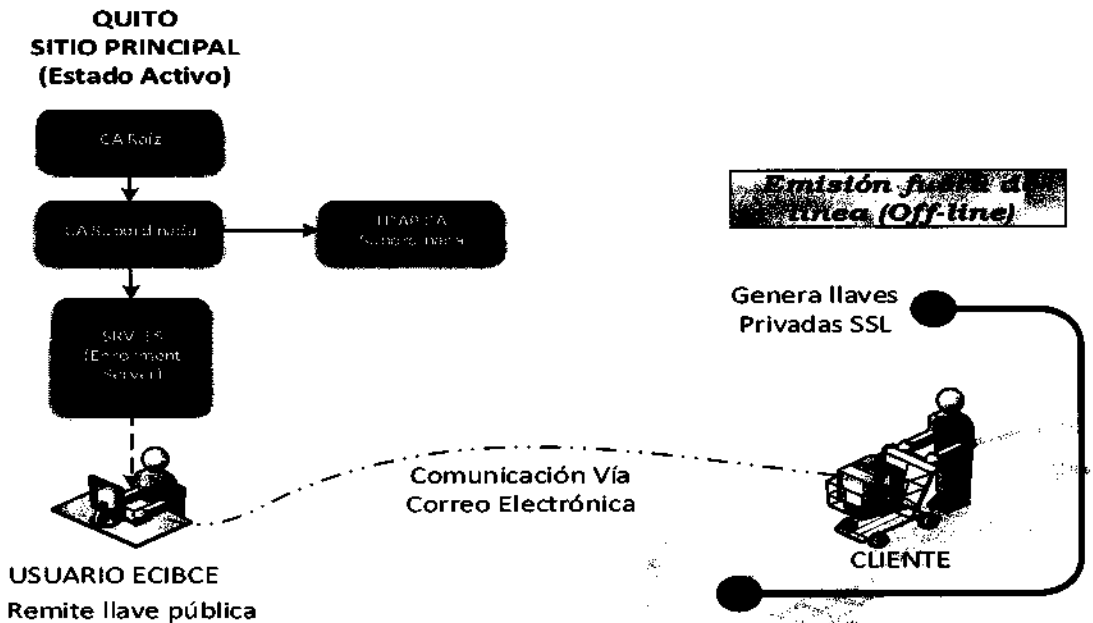
Al ser un Certificado Digital el suscriptor (El representante legal de la empresa, La persona de contacto, el técnico responsable del certificado, la AR que tramitó la solicitud del

certificado.) en caso de pérdida, compromiso de claves u otras causas descritas en la DPC ***ANEXO A.***, deberá solicitar la **revocación** de su certificado.

Igualmente, se publicará la **revocación** del Certificado SSL en la Lista de Certificados revocados (CRL).

Para la **renovación** del certificado SSL la ECIBCE envía notificaciones al contacto técnico registrado en el formulario de solicitud, el certificado se puede renovar si el certificado está vigente, o sesenta (60) días antes de caducado y no debe estar revocado, la duración de este certificado es dos años a partir de su fecha de emisión.

Arquitectura SSL de la ECIBCE



Arquitectura SSL de la ECIBCE

El servicio de emisión de certificados digitales SSL entregado por el Banco Central de Ecuador de acuerdo al gráfico antes señalado esta compuesto en el sitio principal Quito por un nodo activo.

Este servicio esta sobre infraestructura de alta gama en servidores de tipo cuchuilla (blades) de altas prestaciones y en modo cluster, a fin de garantizar los servicios de manera continua y permanente.

14. SERVICIOS DE EMISIÓN, RENOVACIÓN Y REVOCACIÓN DE CERTIFICADOS DIGITALES

La ECIBCE tiene como producto la generación de certificados digitales de firma electrónica para los usuarios finales en diferentes contenedores: Token, Archivo, Roaming, HSM y dispositivo móvil (celular inteligente), para los cuales se efectúan los servicios de emisión, renovación y revocación de los mismos, estos servicios se sustentan en la infraestructura de clave pública de la Entidad de Certificación.

Dirección: Av. Diego de Almagro N31-95 entre Whymper y Alpallana • **Código Postal:** 170518 / Quito - Ecuador • **Teléfono:** 593-2 294-780
www.arcotel.gob.ec

La emisión de los certificados digitales de firma electrónica se realiza para dos tipos de persona: Natural y Jurídica.

Obtención del Certificado Digital de Persona Natural

Para obtener el certificado digital tipo persona natural deberá presentar los siguientes requisitos:

Requisitos del Solicitante Personal Natural

Para ser solicitante y, de ser el caso, posteriormente suscriptor de este tipo de certificados, el solicitante o el suscriptor deben presentar la siguiente documentación:

a) Digitalizado a color de la cédula o pasaporte.
b) Digitalizado de la papeleta de votación actualizada para ecuatorianos, (excepto personas de la tercera edad, los integrantes de las Fuerzas Armadas y Policía Nacional, y las personas con discapacidad. Los ecuatorianos que habitan en el exterior, en caso de no tener la papeleta física, se acogerán a lo que determine el Consejo Nacional Electoral en este ámbito).
c) Digitalizado de la factura de luz, agua o teléfono de los últimos tres meses que certifique la dirección domiciliaria.

Obtención del Certificado de Persona Jurídica

Previo a la solicitud del certificado digital, es importante que la empresa o la organización a la que pertenece el solicitante se encuentre registrada en el Sistema de Certificación Electrónica a través Portal web "*https://www.eci.bce.ec/web/guest/registro-empresa-u-organizacion*" del Banco Central del Ecuador, una vez aprobado el registro podrá solicitar el certificado de persona jurídica.

Requisitos para registrar la Empresa

a) Digitalizado del registro único de contribuyentes (RUC) de la empresa u organización.
b) Digitalizado del nombramiento del representante legal, (de existir delegación o poder subir adjunto al nombramiento, en el mismo documento PDF).
c) Digitalizado de la cédula o pasaporte a color del Representante Legal.

Requisitos del Solicitante Persona Jurídica

Para ser solicitante y, en su caso, posteriormente ser suscriptor de este tipo de certificados, el solicitante o el suscriptor deben poseer la siguiente documentación:

a) Digitalizado a color de la cédula o pasaporte.
b) Digitalizado de la papeleta de votación actualizada para ecuatorianos, (excepto personas mayores de la tercera edad, las ecuatorianas y ecuatorianos que habitan en el exterior, los integrantes de las Fuerzas Armadas y Policía Nacional, y las personas con discapacidad).
c) Digitalizado del nombramiento o certificado laboral (actualizado), que certifique el cargo de la persona, firmado por el representante legal o emitida por el departamento de recursos humanos de la entidad solicitante.
d) Autorización firmada por el representante legal donde conste nombre y cargo de todos los solicitantes de la Empresa para emisión de certificado de Firma Electrónica. (En caso de subrogación, encargo o delegación, adjuntar al oficio el documento de subrogación, encargo o delegación).

Emisión del Certificado Digital

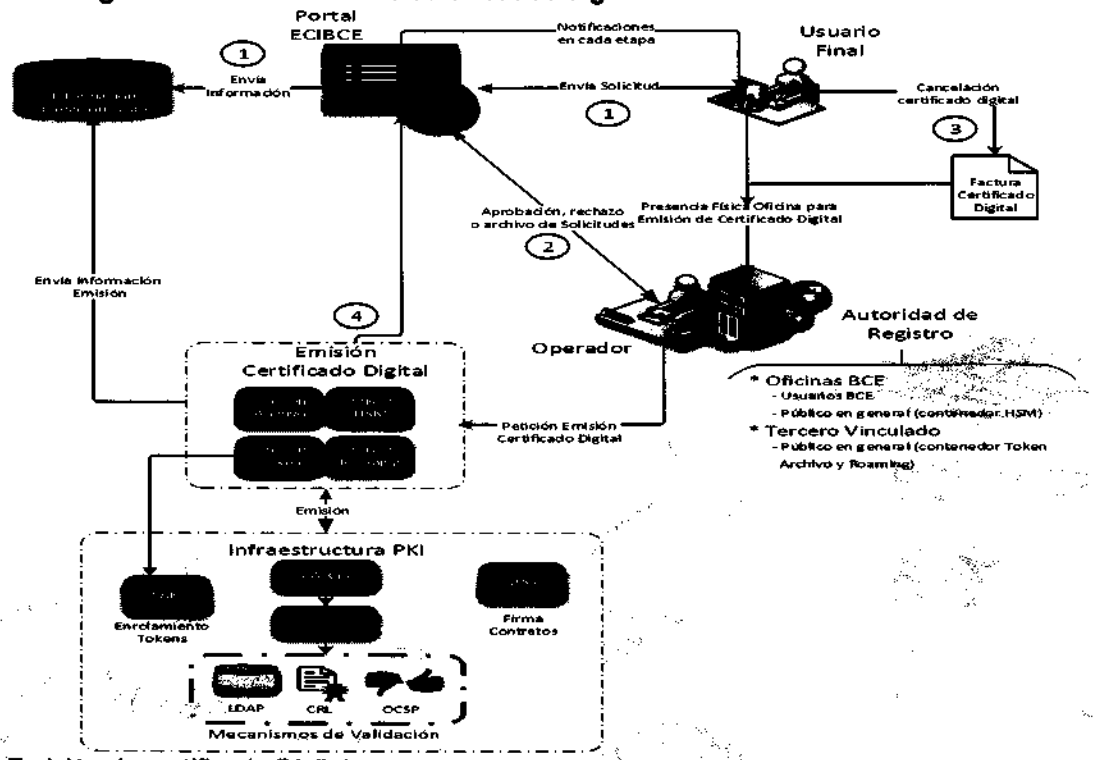
Dirección: Av. Diego de Almagro N31-95 entre Whymper y Alpallana • **Código Postal:** 170518 / Quito - Ecuador • **Teléfono:** 593-2 294-780
www.arcotel.gob.ec

La emisión del certificado digital es el procedimiento mediante el cual se genera el certificado con los datos del suscriptor que lo solicita sea una persona natural o jurídica de manera presencial a fin de validar y verificar la identidad del solicitante el procedimiento de emisión es personal e intransferible y da fe del solicitante para más información refiérase a la DPC ***Anexo A***.

La emisión certifica que el certificado emitido por una AC es fiable y de confianza, estos certificados digitales se pueden emitir en diferentes contenedores para el caso de la ECIBCE se dispone de la emisión en los siguientes contenedores con una vigencia de 2 años:

- Token
- Archivo
- HSM
- Roaming
- Dispositivo móvil (celular inteligente)

Detalle gráfico de la emisión de certificados digitales:



Emisión de certificado Digital

- **(1)** El solicitante accede al portal WEB de la Entidad de Certificación de Información del Banco Central del Ecuador, registra toda la información requerida en el formulario de solicitud de persona natural o de persona jurídica, y sube a la web en formato electrónico toda la información requerida al enviar la solicitud la información se registra a nivel de base.
- **(2)** El responsable del registro o quien cuente con el perfil respectivo, en la ECIBCE o su Tercero Vinculado; verificará meticulosamente la información consignada. En caso de que ésta NO sea correcta, se rechazará la solicitud, se le requerirá subsanar los errores correspondientes y deberá ingresar una nueva solicitud. La respuesta de aprobación o rechazo, se notificará al correo registrado del solicitante/suscriptor quien debe realizar el pago.

- **(3)** Una vez realizado el pago por cualquiera de los medios señalados en la página web de la ECIBCE, el sistema emitirá un correo electrónico al solicitante/suscriptor para que se presente con el documento de identificación, sea éste cédula o pasaporte válido y suficientemente claro y actualizado para permitir su inequívoca identificación, ante la Autoridad de Registro de la ECIBCE o el Tercero Vinculado.
- **(4)** Identificado el suscriptor, la AR confrontará los documentos digitales y los originales aportados, y en caso de ser conformes procederán a la emisión del certificado a nivel de la infraestructura PKI y la información de la emisión será registrada a nivel de base de datos y se mostrará en el sistema de certificación, el proceso de emisión del certificado digital termina con la firma electrónica / digital del contrato y la solicitud registrada.

Nota: Para la emisión en HSM se requerirá adicionalmente la participación de un delegado técnico del suscriptor y la interacción a través del correo electrónico con el personal técnico de ECIBCE.

En Dispositivos criptográficos seguros, tipo TOKEN

Certificado en contenedor Token es un certificado emitido en un dispositivo criptográfico USB, que cumple con los niveles de seguridad FIPS definidos en la DPC, donde se almacena el certificado digital de forma segura.

El dispositivo criptográfico Token está protegido con una clave (PIN) asignada por el usuario dueño del dispositivo, que le permite efectuar operaciones de firma de documentos o transacciones electrónicas, para su emisión se deben efectuar los siguientes pasos:

- El responsable de emisión de la AR introduce en el puerto de su equipo, el dispositivo criptográfico del solicitante, y da inicio al procedimiento de emisión del certificado digital y se ejecuta las siguientes operaciones en el módulo de validación y emisión de certificados:

  - ✓ Genera automáticamente la clave privada en el dispositivo criptográfico.
  - ✓ Envía el CSR (Petición de firma del certificado) a la AC donde se firmará en modo en línea (online).
  - ✓ El certificado es devuelto por la AC e instalado en el dispositivo.

En Dispositivos criptográficos seguros, tipo HSM (Hardware Security Module)

Certificado en dispositivo criptográfico seguro es un certificado de firma electrónica emitido para un contenedor HSM (Hardware Security Module), ideal para altos volúmenes de transacciones, para su emisión se deben efectuar los siguientes pasos:

- La AR verificará el tipo de HSM en la que se emitirá el certificado.
- El responsable de emisión de la AR establece el mecanismo de emisión y validación del certificado, que será asignado al solicitante.
- El módulo de validación y emisión de Certificados ejecuta las siguientes operaciones:

  - ✓ Genera la clave privada en el HSM de manera fuera de línea (offline).
  - ✓ Se envía el CSR (Petición de firma del certificado) a la AC donde se firmará en modo offline.
  - ✓ El certificado es devuelto por la AC e instalado en el HSM.

En Archivo

Certificado en contenedor Archivo es un certificado estándar x.509 en formato p12, que puede ser integrado en cualquier sistema operativo, ideal para realizar transacciones de forma masiva, se lo puede colocar en un servidor o en computador. El usuario debe proteger en

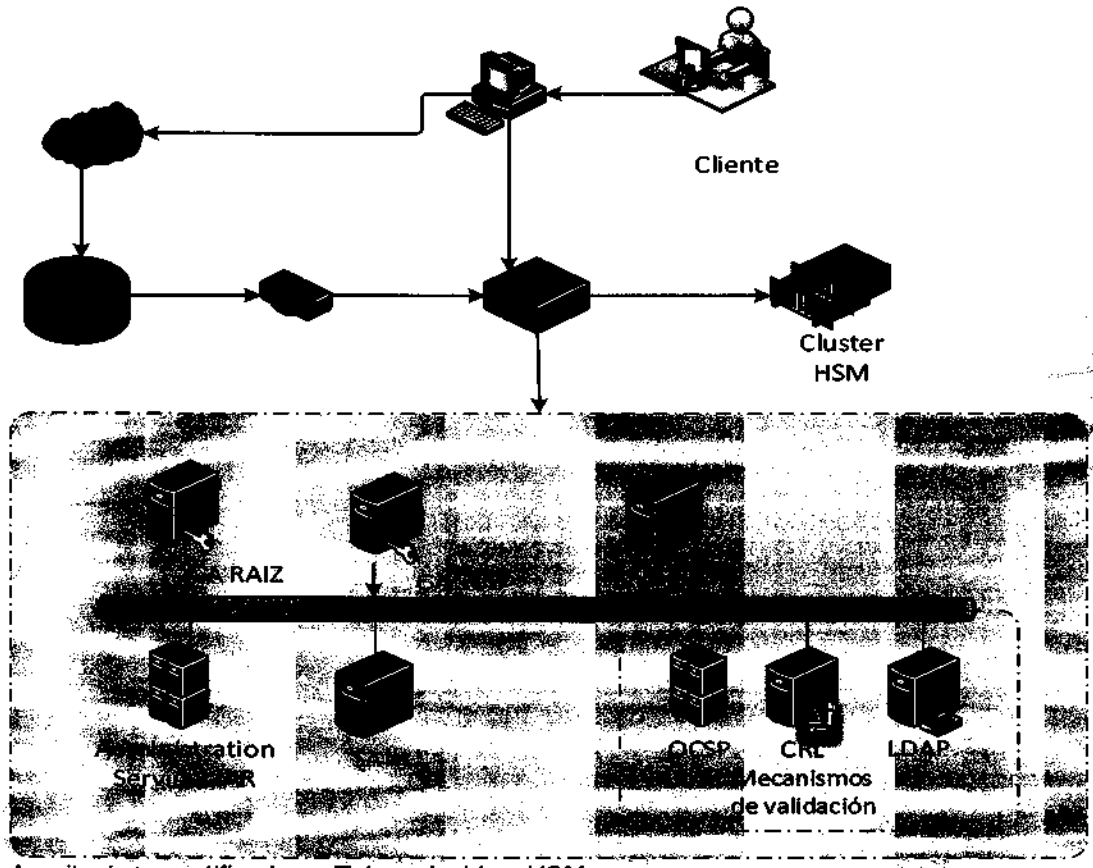
Dirección: Av. Diego de Almagro N31-95 entre Whymper y Alpallana • **Código Postal:** 170518 / Quito - Ecuador • **Teléfono:** 593-2 294-780
www.arcotel.gob.ec

todo momento dicho archivo y las copias que realice del mismo, el certificado posee una clave acceso, para su emisión se deben efectuar los siguientes pasos:

- El responsable de emisión de la AR establece el mecanismo de emisión y validación del certificado, que será asignado al solicitante.
- El módulo de validación y emisión de Certificados ejecuta las siguientes operaciones:

  - ✓ Genera automáticamente la clave privada en el equipo asignado para la emisión.
  - ✓ Desde el equipo asignado se envía el CSR (Petición de firma del certificado) a la AC donde se firmará en modo en línea (online).
  - ✓ El certificado es devuelto por la AC al equipo asignado.

Arquitectura Certificados en contendor Token, Archivo, HSM



Arquitectura certificado en Token, Archivo, HSM

Los certificados digitales emitidos en Token, Archivo y HSM consumen servicios de la infraestructura de clave pública de la ECIBCE, con el fin de generar el conjunto de llaves pública y privada.

Los componentes asociados para la emisión en dispositivos Token, Archivo y HSM son:

- *Administración Plataforma PKI (Administration Service)* permite el registro de los suscriptores para la obtención de los códigos de seguridad para el proceso de emisión (Número de referencia y código de autorización)

Dirección: Av. Diego de Almagro N31-95 entre Whymper y Alpallana • Código Postal: 170518 / Quito - Ecuador • Teléfono: 593-2 294-780
www.arcotel.gob.ec

- *Enrolamiento e Inventario de Token (SAM)* permite el enrolamiento de los dispositivos criptográficos Token a través del número único asociado al suscriptor, además inventariar los tokens a fin de identificar los dispositivos asociados a un suscriptor.
- *Software para firma masiva de documentos (PAS)* permite efectuar de forma masiva y automática la acción de la firma electrónica en los contratos y adendums asociados a los certificados digitales emitidos.

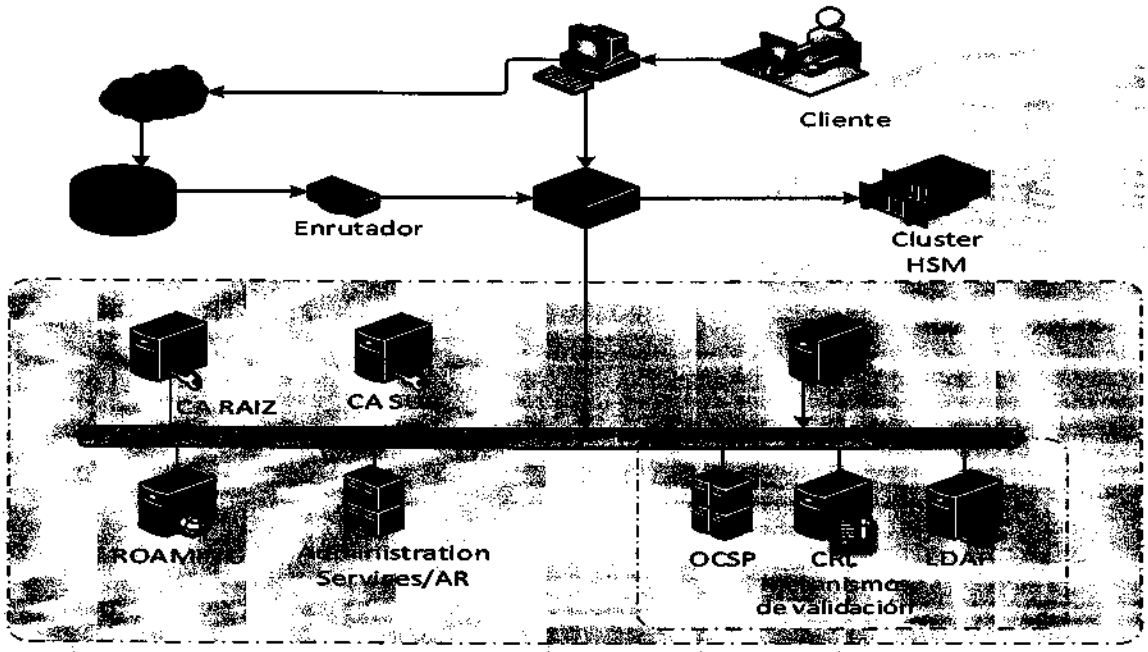
En Roaming

Certificado en contenedor Roaming es un certificado almacenado de forma segura en servidores de la ECIBCE, que le permite realizar operaciones mediante el uso del componente (applet) publicado por la ECIBCE- ROAMING o un aplicativo opcional llamado ESP), para su emisión se deben efectuar los siguientes pasos:

- El responsable de emisión de la AR establece el mecanismo de emisión y validación del certificado, que será asignado al solicitante.
- El módulo de validación y emisión de Certificados ejecuta las siguientes operaciones:

  - ✓ Genera automáticamente la clave privada en el servidor Roaming destinado para la emisión.
  - ✓ Desde el servidor asignado se envía el CSR (Petición de certificado) a la AC donde se firmará en modo en línea (online).
  - ✓ El certificado es devuelto por la AC al servidor (equipo) asignado.

Arquitectura Certificados Roaming



Arquitectura certificado en contenedor Roaming

Los certificados digitales emitidos en Roaming consumen servicios de la infraestructura de clave pública de la ECIBCE, con el fin de generar el conjunto de llaves pública y privada, y el suscriptor puede hacer uso del mismo mediante los siguientes medios de autenticación:

- Mediante un componente (applet) desarrollado por el BCE que permite trabajar con plataformas WINDOWS utilizando un mecanismo de autenticación a través del uso de un usuario y contraseña, este componente se localiza en el portal web de la ECIBCE en la siguiente dirección web: "https://www.eci.bce.ec/conexion-certificados-roaming".

- Mediante un software cliente ESP (Entrust Security Provider) entregado por el BCE que permite trabajar con plataformas WINDOWS y MAC utilizando un mecanismo de autenticación a través del uso de un usuario y contraseña.

Los componentes asociados para la emisión en contenedor Roaming son:

- *Administración Plataforma PKI (Administration Service)* permite el registro de los suscriptores para la obtención de los códigos de seguridad para el proceso de emisión (Número de referencia y código de autorización)
- *Contenedor de Certificados Roaming (Servidor Roaming)* permite crear y custodiar el certificado digital con atributos tipo roaming, el usuario puede accedes a la llave a través de los medios de autenticación previamente mencionas.
- *Software para firma masiva de documentos (PAS)* permite efectuar de forma masiva y automática la acción de la firma electrónica en los contratos y adendums asociados a los certificados digitales emitidos.

Dispositivo móvil (celular inteligente)

El mecanismo para proceder con la emisión y entrega del certificado en este tipo de contenedor, se lo dará a conocer una vez que el servicio esté disponible.

Entrega Certificado Digital

Una vez emitido el certificado digital es entregado al suscriptor, el mismo que debe comprobar en la propia AR que los datos del certificado son correctos y que corresponden a los suyos.

La AR y el suscriptor deben firmar electrónicamente la solicitud y el contrato de prestación de servicios de la ECIBCE en el que se consigna fecha de la entrega.

La AR almacena el contrato y la solicitud en el gestor documental correspondiente y remite al suscriptor vía correo electrónico los archivos firmados electrónicamente.

Revocación del Certificado

Revocar un certificado es anular su validez antes de la fecha de caducidad que consta en el mismo, puede ser solicitada en cualquier momento y en especial, cuando el titular crea que sus claves privadas son conocidas por otros, la revocación se efectúa de igual forma tanto a personas naturales como a jurídicas.

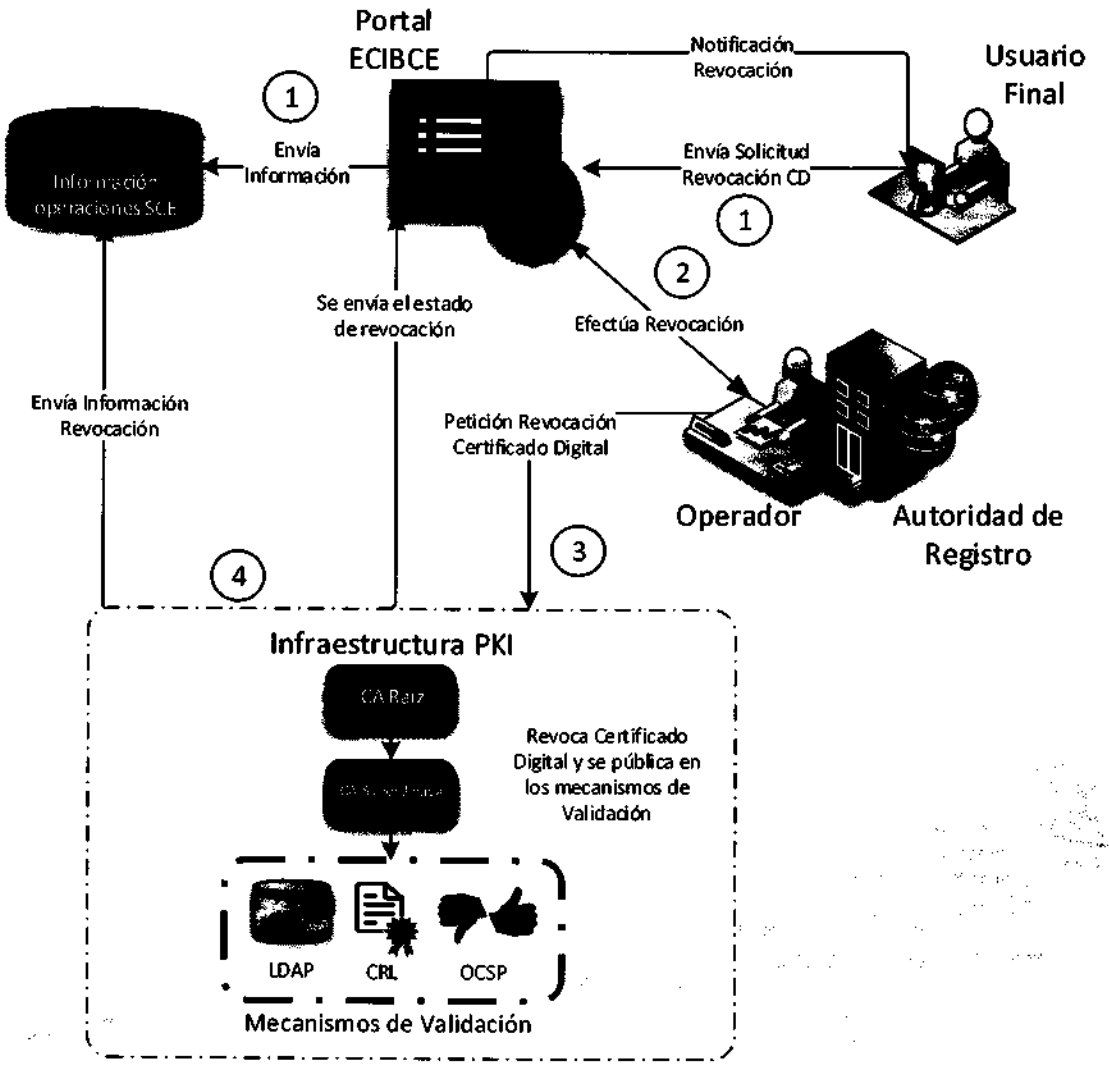
La revocación tiene efectos a partir de la fecha efectiva de revocación del certificado digital cuyos números de series se reflejan en las listas de certificados revocados publicados por la Autoridad de Certificación, cualquier firma digital realizada con la clave privada asociada a ese certificado con posterioridad a la fecha efectiva de revocación no tendrá validez.

Supuestos y efectos de revocación:

Los Certificados de Persona Natural y Jurídica deberán ser revocados cuando concurra alguna de las circunstancias determinadas en las políticas de certificados (PC) respectivamente y tendrán efectos de revocación acorde a lo expuesto en los mismas PCs.

Dirección: Av. Diego de Almagro N31-95 entre Whymper y Alpallana • **Código Postal:** 170518 / Quito - Ecuador • **Teléfono:** 593-2 294-780
www.arcotel.gob.ec

6.1.1. **Detalle gráfico de la revocación de certificados digitales:**



Revocación de certificado Digital

- **(1)** Usuario Final (solicitante/suscriptor) del Certificado de Persona Natural o Jurídica; o el Representante Legal en caso de que el suscriptor no lo pueda hacer (aplica para Persona Jurídica), así como también la AR relacionada a aquellos certificados en cuya emisión haya participado), solicitarán la revocación llenando el formulario correspondiente en el portal de Certificación Electrónica (que efectuará el respectivo registro a nivel de base de datos), en cuanto tengan conocimiento de la concurrencia de alguna de las circunstancias determinadas y detalladas en las políticas de certificados (PC).

- **(2)** Una vez recibida y verificada la solicitud de revocación, la AR procederá a tramitar la revocación efectiva del certificado

- **(3)** En la infraestructura PKI se realiza el proceso de revocación que incluye la anulación de las llaves asociadas al certificado digital, esta información es replicada a los mecanismos de validación del certificado digital (CRL, OCSP,LDAP).

Dirección: Av. Diego de Almagro N31-95 entre Whymper y Alpallana • **Código Postal:** 170518 / Quito - Ecuador • **Teléfono:** 593-2 294-780
www.arcotel.gob.ec

- **(4)** La información del certificado revocado se refleja a nivel de la Base de Datos y en el portal de la Entidad de Certificación, una vez finalizado el proceso de revocación se envía al suscriptor una notificación vía correo electrónico a la dirección consignada en la petición del certificado.

La información relativa al estado de la revocación estará disponible las 24 horas del día, los 7 días de la semana. En caso de fallo del sistema, servicio o cualquier otro factor que no esté bajo el control de la ECIBCE.

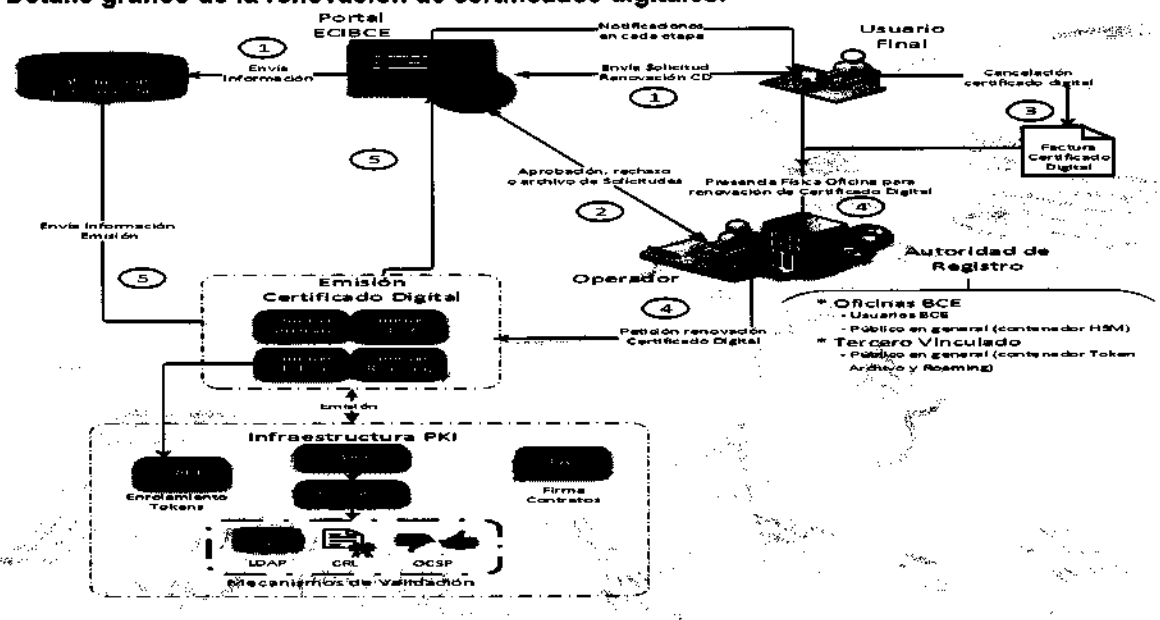
Renovación del Certificado

Este procedimiento se establece para los casos en que el certificado vaya a caducar y el suscriptor simplemente desee utilizar un certificado con las mismas características que tenía el que venía utilizando válidamente hasta entonces.

En este caso, la ECIBCE generará nuevas claves; pero, únicamente se van a llevar a cabo unas medidas mínimas de comprobación de datos, puesto que el antiguo certificado tiene plena vigencia y nada hace pensar que alguno de sus datos ha cambiado o que ya no es posible confiar en el certificado.

Los certificados emitidos por la ECIBCE tienen un plazo de vigencia establecido en el propio certificado y siempre será acorde con la legislación vigente. La renovación de los certificados digitales podrá ser realizada siempre y cuando cumpla los requisitos expuestos en las políticas de certificados (PC).

Detalle gráfico de la renovación de certificados digitales:



Renovación de certificado Digital

- **(1)** El solicitante accede al portal WEB de la Entidad de Certificación de Información del Banco Central del Ecuador, registra toda la información requerida en el formulario de solicitud correspondiente, sube a la web los documentos habilitantes requeridos en formato electrónico al enviar la solicitud la información se registra a nivel de base.
- **(2)** El responsable del registro o quien cuente con el perfil respectivo, en la ECIBCE o su AR; verificará meticulosamente la información consignada. En caso de que ésta NO sea correcta, se le rechazará y se le requerirá subsanar los errores correspondientes e ingresará una nueva solicitud. En caso de que sea aprobada, se notificará al correo del solicitante/suscriptor registrado, quien debe realizar el pago.

Dirección: Av. Diego de Almagro N31-95 entre Whymper y Alpallana • **Código Postal:** 170518 / Quito - Ecuador • **Teléfono:** 593-2 294-780
www.arcotel.gob.ec

- **(3)** Una vez registrado y realizado el pago por cualquiera de los medios habilitados, el sistema emitirá un correo electrónico al solicitante/suscriptor para que se presente con el documento de identificación, sea éste cédula o pasaporte válido y suficientemente claro y actualizado para permitir su inequívoca identificación, ante la Autoridad de Registro de la ECIBCE.
- **(4)** Identificado el suscriptor, la AR confrontará los documentos digitales y los originales aportados, y en caso de ser conformes procederán a la renovación del certificado digital a nivel de la infraestructura PKI.
- **(5)** La información del certificado renovado se refleja a nivel de la Base de Datos y en el portal de la Entidad de Certificación, una vez finalizado el proceso de renovación se efectuará la firma del contrato y de la solicitud registrada.

Validez del Certificado de Firma Electrónica de Persona Natural y Jurídica

El período de validez o vigencia máximo del Certificado de Firma Electrónica de Persona Natural y Jurídica es de dos años desde su emisión en cualquier tipo de contenedor (Token, HSM, Archivo o Roaming o dispositivo móvil tipo Smartphone), pasado este periodo pierde su vigencia.

Un Certificado que ha perdido su vigencia, se considera caducado, por lo que pierde su validez y no podrá ser utilizado por el suscriptor.

Los certificados caducados se reflejarán en la lista de certificados revocados – CRL, y serán publicados en el portal web de la ECIBCE.

Aceptación de Certificados

La entrega del certificado y la firma del contrato implicarán la aceptación del certificado por parte del suscriptor. La aceptación del certificado deberá realizarse de forma expresa, por escrito y ante el encargado de la ECIBCE o de la AR. El solicitante emitirá esta aceptación en su propio nombre y, en su caso, en nombre y representación de la entidad que vaya a ser vinculada por el propio certificado

No obstante, a partir de la entrega del certificado, el suscriptor dispondrá de dos días laborables para revisar el mismo, determinar si es adecuado y si los datos se corresponden con la realidad. En caso de que existiera alguna diferencia entre los datos suministrados a la ECIBCE y el contenido del certificado, ello deberá ser comunicado de inmediato a la ECIBCE para que proceda a su revocación y a la emisión de un nuevo certificado. La ECIBCE entregará el nuevo certificado sin costo para el usuario en el caso de que la diferencia entre los datos sea causada por un error no imputable al suscriptor. Transcurrido dicho periodo sin que haya existido comunicación, se entenderá que el suscriptor ha confirmado la aceptación del certificado y de todo su contenido.

Aceptando el certificado, el suscriptor confirma y asume la exactitud del contenido del mismo, con las consiguientes obligaciones que de ello se deriven frente a la AR, la ECIBCE o cualquier tercero que de buena fe confíe en el contenido del Certificado.

Firma y entrega del contrato

El suscriptor debe comprobar en la propia AR que los datos del certificado son correctos.

La AR y el suscriptor deben firmar de manera electrónica la solicitud y el contrato de prestación de servicios de la ECIBCE en el que se consigna fecha y hora de la entrega. Estos documentos se remitirán vía correo electrónico al usuario; y la AR archivará una copia.

Dirección: Av. Diego de Almagro N31-95 entre Whymper y Alpallana • **Código Postal:** 170518 / Quito - Ecuador • **Teléfono:** 593-2 294-780
www.arcotel.gob.ec

La AR realizará la entrega física del certificado digital de acuerdo al tipo de contenedor solicitado en el que está el certificado, al usuario o a una tercera persona, siempre y cuando presente un poder notarizado.

15. AUTORIDADES DE REGISTRO (AR)

La ECIBCE actualmente posee dos Autoridades de Registro, Banco Central del Ecuador y Registro Civil como Tercero Vinculado, que permiten cubrir geográficamente la entrega de los servicio de Certificación Electrónica. Estas Autoridades permiten validar la identidad de los solicitantes y emitir el certificado digital de firma electrónica.

La ECIBCE se reserva el derecho a asumir con previo aviso cualquier parte de los servicios de certificación que preste el Tercero Vinculado o a revocar o suspender cualquiera de los Certificados emitidos, si ello resulta necesario para preservar la seguridad del sistema de certificación.

A continuación se detalla una breve descripcion del modo de operación de la Autoridades de Registro de la ECIBCE:

AR del Banco Central del Ecuador:

La AR del Banco Central del Ecuador permite brindar atención a los funcionarios del Banco Central en la emisión, renovación y revocación de certificados digitales de firma electrónica de Persona Natural y Jurídica del BCE, certificados digitales SSL para las Páginas Web internas del BCE, y para las entidades financieras que interactúan con el Sistema Nacional de Pagos para comunicación segura punto a punto.

Así tambien realiza la emisión de certificados digitales de firma electrónica en contenedor HSM y genera los planes de Sellado de Tiempo para usuarios finales a nivel nacional.

Funciones

La AR del Banco Central del Ecuador cumple las funciones señaladas en la DPC, para la gestión de certificados digitales de firma electrónica, en este ámbito son las siguientes:

Para Funcionarios del BCE:

- Emisión y renovación de certificados digitales en Token, formato PKCS#11.
- Emisión y renovación de certificados digitales en Archivo, formato PKCS#12.
- Emisión y renovación de certificados digitales en modalidad Roaming.
- Servicio de revocación de certificados digitales.

Para Uso del Banco Central y entidades relacionadas al Sistema Nacional de Pagos:

- Emisión y renovación de certificados digitales SSL.

Para Público en General:

- Emisión y renovación de certificados digitales en HSM.
- Generación de planes de sellado de tiempo
- Soporte informativo al usuario.

Para brindar los servicios antes mencionados la AR del Banco Central del Ecuador dispone de 3 agencias de atención a nivel nacional:

- Edificio Matríz Quito,
- Dirección Zonal Guayaquil, y;
- Dirección Zonal Cuenca

Dirección: Av. Diego de Almagro N31-95 entre Whymper y Alpallana • **Código Postal:** 170518 / Quito - Ecuador • **Teléfono:** 593-2 294-780
www.arcotel.gob.ec

1	PICHINCHA	Quito	(02) 3938600	2858 / 2994	Av. 10 de Agosto N11-409 y Briceño
2	GUAYAS	Guayaquil	(04) 2729470	[illegible]	[illegible]
3	CUENCA	Cuenca	(07) 2831255	7214	Calle Larga y Huaynacapac

Cobertura de Emisión de la Autoridad de Registro BCE

AR Tercero Vinculado (Registro Civil):

La AR del Registo Civil permite brindar atención al público en general con cobertura a nivel nacional para la emisión, renovación y revocación de certificados digitales de firma electrónica de personas naturales y jurídica, en contenedores Token, Archivo o Roaming.

La prestación de los servicios de certificación podrá ser proporcionada por un tercero vinculado contractualmente con una Entidad de Certificación de Información y servicios relacionados Acreditada, con sujeción a lo dispuesto en el artículo 33 de la Ley de Comercio Electrónico, firmas y mensaje de datos y artículo innumerado "Terceros Vinculados" del Reglamento a la Ley de Comercio Electrónico.

El 25 de febrero de 2014 el Banco Central del Ecuador y la Dirección General de Registro Civil, Identificación y Cedulación suscribieron el "Contrato de Tercero Vinculado" para la gestión de certificados digitales de firma electrónica; en tal sentido sus funciones y obligaciones son las siguientes:

Funciones

El Tercero Vinculado deberá cumplir las funciones de Autoridad de Registro, señaladas en la DPC ***Anexo A***, para la gestión de certificados digitales de firma electrónica, en este ámbito son las siguientes:

- Emisión y renovación de certificados digitales en Token, formato PKCS#11.
- Emisión y renovación de certificados digitales en Archivo, formato PKCS#12.
- Emisión y renovación de certificados digitales en modalidad Roaming.
- Servicio de revocación de certificados digitales.
- Soporte informativo al usuario.

El Tercero Vinculado asumirá las responsabilidades y obligaciones descritas en el Contrato de Tercero Vinculado.

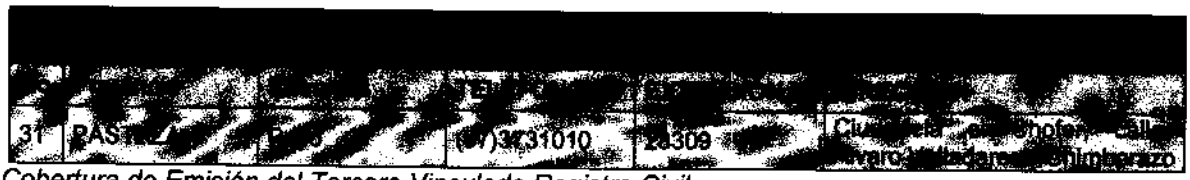
El Tercero Vinculado, en la actualidad cuenta con 31 agencias a nivel nacional, las mismas que detallamos a continuación:

No.					
1	AZUAY	Cuenca	(07)3700990	1314	Alfonso Jerves y Manuel Vega
2	BOLÍVAR	[illegible]	[illegible]	[illegible]	[illegible]
3	CAÑAR	Azogues	(07)3701190	3309	Solano 3-07 entre Matovelle y Rivera
4	CARCHI	[illegible]	[illegible]	[illegible]	[illegible]
5	COTOPAXI	Latacunga	(03) 3731030	6306	Hermanos del Buen Pastor y Madres Oblatas

[redacted]

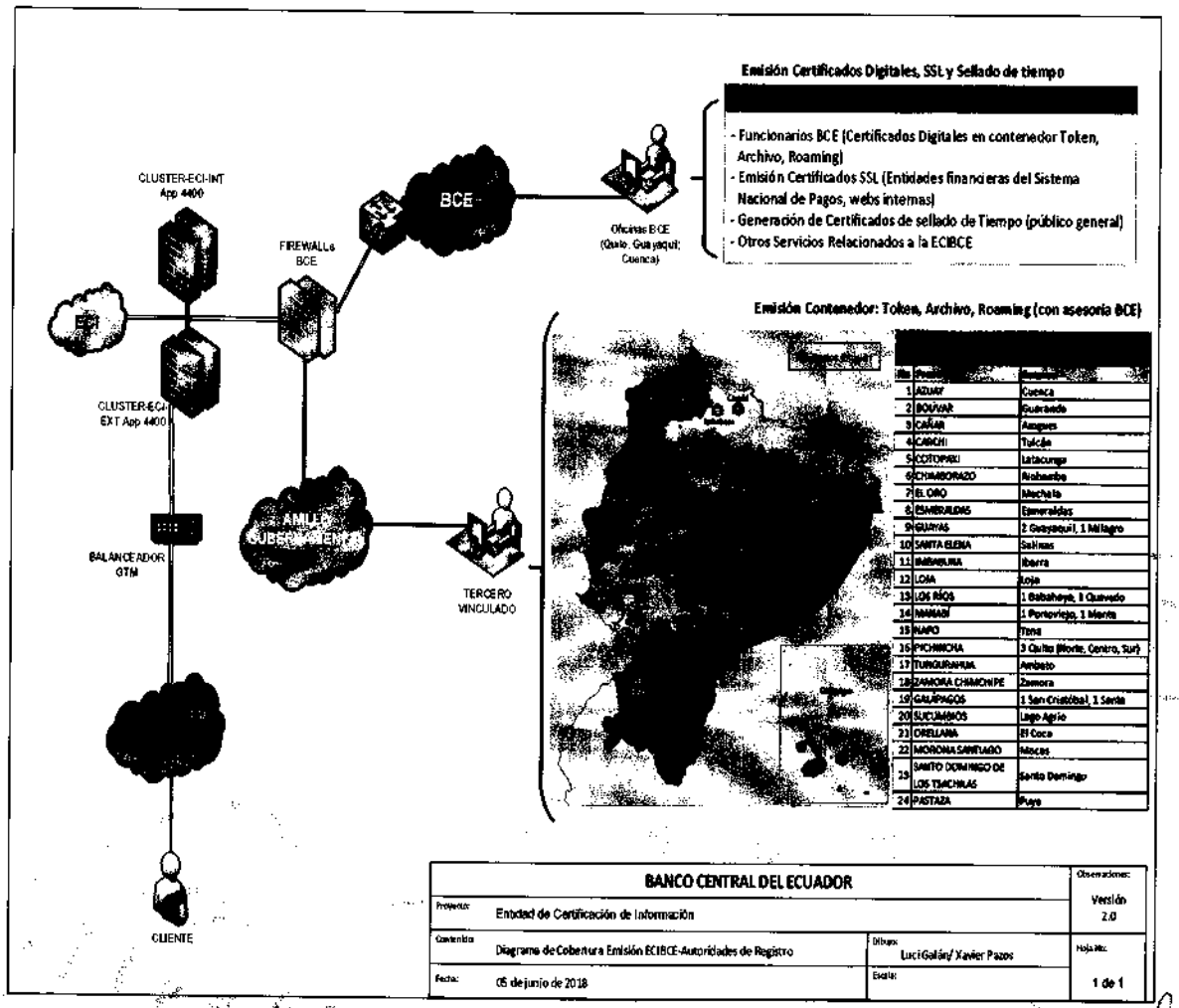
[redacted]					
7	EL ORO	Machala	(07)3701000	7316	Av. 25 de junio entre Juan Montalvo y 9 de mayo
[redacted]					
9		Guayaquil Sur	(04)3712260	11303	Av. 25 de julio y Av. Los Esteros, esquina
10	GUAYAS	Guayaquil Centro	(04)2592470	10106/10124	Pedro Carbo 505 y Av. 9 de octubre
11		Milagro	(04) 2592470	10357	Av. Cristóbal Colón y 17 de septiembre (CAC Centro de Atención Ciudadana)
[redacted]					
13	IMBABURA	Ibarra	(06)3731000	16312	Calle Juan de Velasco y Rocafuerte
[redacted]					
15	LOS RÍOS	Babahoyo	(05)3700995	18401	27 de Mayo y Segunda calle, Sector 5 esquinas
16		Quevedo	(05)3700995	19307/19309	San Camilo Pro mejoras, calle entre la H y la Y
[redacted]					
19	NAPO	Tena	(06)3731010	25310	Calles Chonta Yacu entre Fausto Castello y Gabriel Espinoza, Barrio las Orquídeas
[redacted]					
23	TUNGURAHUA	Ambato	(03)3731040	37319	Ernesto Alvarado y Bolívar Sevilla
[redacted]					
25	GALÁPAGOS	San Cristóbal	(05)2520312	9010	Calle Isabela y Av. Juan José Flores, Isla San Cristóbal
26		Santa Cruz	(05)2520312	9101	Vía Baltra
[redacted]					
28	ORELLANA	El Coca	(06)3731050	26315	Calles Quito entre Pompeya y Primavera
[redacted]					
30	SANTO DOMINGO DE LOS TSACHILAS	Santo Domingo	(02)3730790	35315	Av. Clemencia de Mora y Av. Esmeraldas

Dirección: Av. Diego de Almagro N31-95 entre Whymper y Alpallana • Código Postal: 170518 / Quito - Ecuador • Teléfono: 593-2 294-780
www.arcotel.gob.ec



Cobertura de Emisión del Tercero Vinculado Registro Civil

A continuación se muestra el diagrama de cobertura de Emisión de Certificados Digitales a través de las oficinas de la AR, tanto del BCE como del Tercero Vinculado (Registro Civil):



Dirección: Av. Diego de Almagro N31-95 entre Whymper y Alpallana • **Código Postal:** 170518 / Quito - Ecuador • **Teléfono:** 593-2 294-780
www.arcotel.gob.ec

INFORME TÉCNICO – ECONÓMICO/FINANCIERO – JURÍDICO	
Nro.	INFORME No. CTDS-OTH-EC-2018-0237
Tipo:	Técnico Económico Jurídico.
Fecha:	22 de octubre de 2018

El Banco Central del Ecuador el 06 de julio de 2018, ingresó a la Agencia de Regulación y Control de las Telecomunicaciones ARCOTEL, el Oficio Nro. BCE-BCE-2018-0465-OF solicitando la renovación de la Acreditación como Entidad de Certificación de Información y Servicios Relacionados.

El presente informe incluye cuatro secciones donde se contempla:

- SECCIÓN I: Informe Técnico
- SECCIÓN II Informe Económico
- SECCIÓN III: Informe Jurídico

ANTECEDENTES

1. El Banco Central del Ecuador es una Entidad de Certificación de Información y Servicios Relacionados (ECIBCE) acreditada por el ex Consejo Nacional de Telecomunicaciones, mediante Resolución 481-20-CONATEL-2008 de 08 de octubre de 2008 y acto administrativo suscrito el 6 de noviembre de 2008.

2. Con Memorando Nro. ARCOTEL-CTHB-2018-0418-M de 03 de mayo de 2018, la Coordinación Técnica de Títulos Habilitantes solicitó a la Coordinación Técnica de Control, autorice a quien corresponda la emisión de los informes de Quito y Guayaquil de la operación y prestación del servicio de la Entidad de Certificación de Información y Servicios Relacionados del Banco Central del Ecuador

1. Con Oficio Nro. BCE-BCE-2018-0465-OF de 06 de julio de 2018, ingresado mediante documento Nro. ARCOTEL-CTDS-2018-0009-E de 06 de julio de 2018, el Banco Central del Ecuador solicitó a la Agencia de Regulación y Control de las Telecomunicaciones, la renovación de la acreditación como Entidad de Certificación de Información y Servicios Relacionados.

2. La Agencia de Regulación y Control de las Telecomunicaciones – ARCOTEL, publicó en la página Web institucional el 26 de julio de 2018, el extracto de la solicitud para la renovación de la acreditación como Entidad de Certificación de Información y Servicios Relacionados a favor del Banco Central del Ecuador. Como resultado de la publicación, la Unidad de Comunicación Social de la ARCOTEL, indicó que no se presentó ninguna observación al respecto.

3. Con Memorando Nro. ARCOTEL-CTHB-2018-0798-M de 08 de agosto de 2018, la Coordinación Técnica de Títulos Habilitantes, realizó la insistencia a la Coordinación Técnica de Control, para que se emitan los informes técnicos de las ciudades de Quito y Guayaquil, relacionados con la operación de la acreditación como Entidad de Certificación de Información y Servicios Relacionados del Banco Central del Ecuador.

4. Con Memorando Nro. ARCOTEL-CCON-2018-0949-M de 21 de agosto de 2018, la Coordinación Técnica de Control, informó a la Coordinación Técnica de Títulos Habilitantes que realizará las gestiones pertinentes ante los organismos desconcentrados de Guayaquil y Quito para la entrega de los informes técnicos de la Entidad de Certificación de Información y Servicios Relacionados del Banco Central del Ecuador.

5. Con Memorando ARCOTEL-CZ05-2018-1552-M de 23 de agosto de 2018, la Coordinación Zonal 5 remitió a la CCDS, el informe técnico IT-CZ05-C-2018-0548 de 20 de agosto de 2018, con los resultados de la inspección efectuada en la ciudad de Guayaquil, provincia de Guayas, a las instalaciones del Banco Central del Ecuador.

6. Con Memorando ARCOTEL-CZ02-2018-1377-M de 14 de septiembre de 2018, la Coordinación Zonal 2, envió a la CCDS, el informe técnico IT-CZ02-C-2018-0946 de 06 de septiembre de 2018, con los resultados de la inspección efectuada en Sangolqui, provincia de Pichincha, a las instalaciones del Banco Central del Ecuador.

7. Con Memorando ARCOTEL-CTDS-2018-0849-M de 17 de septiembre de 2018, la Dirección Técnica de Títulos Habilitantes de Servicios y Redes de Telecomunicaciones, solicitó a la Dirección Técnica de Gestión Económica de Títulos Habilitantes, remita el informe de Obligaciones Económicas del Banco Central del Ecuador, como Entidad de Certificación de Información y Servicios Relacionados.

8. Con Memorando ARCOTEL-CCON-2018-1048-M de 17 de septiembre de 2018, la Coordinación Técnica de Control, remitió el informe técnico de operación sobre la Entidad de Certificación de Información y Servicios Relacionados denominada "Banco Central del Ecuador".

9. Con Memorando Nro. ARCOTEL-CTDG-2018-0530-M de 02 de octubre de 2018, la Dirección Técnica de Gestión Económica de Títulos Habilitantes, envió a la Dirección Técnica de Títulos Habilitantes de Servicios y Redes de Telecomunicaciones, el Informe de Obligaciones Económicas del Banco Central del Ecuador, como Entidad de Certificación de Información y Servicios Relacionados.

SECCIÓN I

INFORME TÉCNICO

INFORME TÉCNICO

1. INTRODUCCIÓN

Con Oficio Nro. BCE-BCE-2018-0465-OF de 06 de julio de 2018, ingresado mediante documento Nro. ARCOTEL-CTDS-2018-0009-E de 06 de julio de 2018, a la Agencia de Regulación y Control de las Telecomunicaciones ARCOTEL, el Banco Central del Ecuador solicito la renovación de la Acreditación como Entidad de Certificación de Información y Servicios Relacionados.

2. DESCRIPCIÓN DE LOS SERVICIOS AUTORIZADOS.

Situación Actual de la Infraestructura PKI del Banco Central del Ecuador

El Banco Central del Ecuador dispone de la infraestructura de clave pública que es un mecanismo que combina hardware, software, políticas y procedimietnos que permiten asegurar la identidad digital de los usuarios internos como externos que consumen certificados digitales, mecanismos de validación planes de sellado de tiempo entre otros, tambien suministra el procedimiento que permite asegurar la identidad digital de los usuarios del sistema Nacional de Pagos que ingresan a través de la red Privada del Sistema Financiero con el uso de certificados digitales que incluyen la firma electrónica.

En el País, la firma electrónica tiene validez jurídica amparada en la ley de Comercio Electronico, firmas Electrónicas y Mensajes de Datos, codificacion N0 202-67 –R.O. Sup 557 – del Miercoles 17 de abril de 2002, y su última modificación del 10 de febrero de 2014 de acuerdo a lo establecido en el Art. 13:

"Firma electrónica.- Son los datos en forma electrónica consignados en un mensaje de datos, adjuntados o lógicamente asociados al mismo, y que puedan ser utilizados para identificar al titular de la firma en relación con el mensaje de datos, e indicar que el titular de la firma aprueba y reconoce la información contenida en el mensaje de datos."

Por tanto el uso de firma electronica se justifica plenamente debido a que en el caso de presentarse una disputa legal, puede comprobarse técnicamente que la firma corresponde a la persona que efectuo la transacción, es decir, la firma es usada como un recurso probatorio.

Adicionalme, la firma electrónica es utilizada como una medida disuasiva, pensada también en la protección del usuario conttra posible ataques y/o fraudes electrónicos.

Por otro lado, el cifrado de datos es una técnica que permite transformar cierta información en una serie de datos ininteligibles o "*datos cifrados*", protegiendo la información contra usuarios no autorizados a accederla, manteniendo de esta manera la confidencialidad de la misma amparada en el Acuerdo Ministerial 166 del 25 de septiembre de 2013 y su última modificación del 15 de junio de 2016.

El siguiente cuadro resume y explica el servicio que brinda la firma electrónica y el cifrado de datos, para su diferenciación.

MECANISMO SEGURIDAD	DE SERVICIO	BASE LEGAL
Cifrado de Datos	Confidencialidad	Esquema Gubernamental de Seguridad de la Información - EGSI
Firma Electrónica	• Autenticidad • Integridad • No repudio o Aceptación	Ley de Comercio Electronico, Firmas Electrónicas y Mensajes de Datos

Descripción detallada del servicio propuesto como entidad de certificación.

Las organizaciones actuales se orientan a la conservacion y respaldo de la información que manejan a través de modelos de seguridad que permite brindar sus servicios de forma confiable con el resguardo de toda informacion sencible considerando mecanismos de identificación, autenicación, autorización, integridad y confidencialidad, en el Ecuador la Ley de Comercio Electronico, Firmas y Mensajes de Datos, regula los mensajes de datos, la firma electrónica, los servicios electrónicos, a través de redes de información, incluido el comercio electronico y la protección de los usuarios de estos sistemas.

De esta manera la Entidad de Certificación de Información del Banco Central a traves del uso de su Infraestructura de Clave Pública – PKI (*Public Key Infraestructure*) permite crear las identidades digitales y la confianza que se necesita para los procesos de identificacion y autenticación asi como la administracion de las claves públicas y privadas de los usuarios. El manejo de los certificados difgitales en conbinacion con las claves públicas y privadas, permite la identificación precisa de los participantes mediante la validacion de su identidad, y el acceso a la información requerida sólo al personal autorizado (control de acceso), asegurando la confidencialidad e integridad de los datos gracias a las técnicas de criptográficas o de cifrado de datos.

El papel primario de la Infraestrutura PKI es establecer identidades digitales confiables entre sus participantes, es decir, el Banco central del Ecuador actúa como el tercero confiable entre las instituciones participantes, ofreciendo un nivel de credibilidad razonable en el proceso que usa para emitir los certificados digitales en conjunción con las claves públicas y privadas, demostrando que la identidad que crea y los mecanismos de identificación que utiliza, son veraces y legalmente aceptados.

La infraestructura PKI requiere de directivas o politicas de seguridad, de software y hardware especializados que permitan la seguridad y facil admiistración, de administradores que soporten todo la infraestructura y atiendan los requerimietnos de los usuarios.

Los componentes tecnológicos de la infraestructura PKI del Banco Central del Ecuador son los siguientes:

Componente	Aplicación	Plataforma
Autoridad de Certificación (AC)	Entrust Authority Security Manager	Red Hat Enterprise Linux 5.4
Autoridad de Certificación Subordinada	Entrust Authority Security Manager	Microsoft Windows Server 2008 R2
Repositorio de Certificados Digitales (LDAP RAIZ)	Open Ldap	Red Hat Enterprise Linux 6.0
Repositorio de Certificados Digitales (LDAP Subordinado)	Open Ldap	Red Hat Enterprise Linux 6.0
Administration Services	Entrust Authority™ Administration	Microsoft Windows Server 2008 R2
Lista de Certificados Revocados	Apache	Red Hat Enterprise Linux 6
Protocolo de comprobación del Estado de un Certificado En línea (OCSP)	3. **OCSP-EJBCA**	Red Hat Enterprise Linux 5.5
Protocolo de comprobación del Estado de un Certificado En línea (OCSP)	4. **KeyOne Validation Authority**	Microsoft Windows Server 2012 R2 Standar
Contenedor Certificado Roaming	Entrust Authority™ Roaming Server	Microsoft Windows Enterprise 2008
Contenedor Certificado Archivo	Entrust Authority™ Digital Identity Manager	Microsoft Windows Server 2008 R2 Enterprise

Componente	Aplicación	Plataforma
Contenedor Certificado Token	Api Generación Certificados en contenedor Token	Solaris 10
Sellado de Tiempo	Ascertia	Microsoft Windows Server 2012 R2 Standar

Adicionalmente, y con el fin de garantizar la disponibilidad de los servicios asociados a la infraestructura PKI, el Banco Central del Ecuador dispone de una arquitectura de alta disponibilidad y desarrolló un plan de contingencia, considerando como sitio alterno a la Dirección Zonal Guayaquil.

Mecanismos de validación: CRL, OCSP, LDAP

La ECIBCE, dispone de mecanismos de validación a traves de la lista de certificados revocados con el fin de mantener la confiabilidad de los certificados emitidos por la Entidad de Certificacion, los mecanismos son:

- Servicio de Listas de Certificados Revocados (CRL)
- Servicio de Consulta en Línea de Certificados Digitales (OCSP)
- Servicio de Repositorio de Certificados Digitales (LDAP)

Sellado de tiempo (TSA – Time Stamp Authority)

Es un servicio que permite asegurar el momento en que un documento electrónico fue creado, es emplear una tercera parte de confianza, comúnmente llamada una autoridad de sellado de tiempo (TSA).

Dentro del proceso de envío y recepción del documento firmado digitalmente con su respectiva fecha y hora el Banco Central actúa como una tercera parte de confianza, comúnmente llamada una autoridad de sellado de tiempo (TSA) para vincular una hora a la firma digital en el momento en que la firma fue creada o cerca de la creación de la misma.

La solución del servicio de sellado de tiempo incluye una aplicación que le permitirá al usuario sellar el documento (hora y fecha) generando una mayor seguridad, garantía y validez al mismo.

Sistema de Tarificación de Servicios de Sellado de Tiempo

El propósito general de TTSA es de servir de intermediario entre un cliente final, que utiliza servicios de sellado de tiempo, y un proveedor de dichos servicios. Al proveedor de los servicios de sellado de tiempo se llama Autoridad de estampado o sellado de tiempo "TSA".

Al ser un intermediario, el TTSA permite tener control sobre todas las peticiones que se envían a la TSA, de manera que puede proveer varios servicios adicionales. Esto implica que se pueden hacer validaciones adicionales sobre quién envía las peticiones, y llevar un registro de todas las estampas firmadas por la TSA.

Certificados de servidor seguro (SSL)

Los Certificados de Servidor Web son certificados expedidos a entidades públicas o privadas para servidores seguros o web. La finalidad del certificado es autenticar de forma segura el servidor en la red y permitir a los usuarios crear una conexión segura mediante protocolos criptográficos estándar, como SSL o TLS. Toda la información contenida en el certificado para servidor seguro es suministrada a la entidad que actúa como Autoridad de Registro por el propio suscriptor bajo su entera responsabilidad.

La información enviada desde un usuario hacia el Servidor Seguro viaja encriptado, por lo que de ser interceptada es imposible de descifrar. Además la información se marca digitalmente, lo que permite verificar si fue alterada en el trayecto que viaja la información.

5. DESCRIPCIÓN TÉCNICA DE LA RED.

El Banco Central del Ecuador como Entidad de Certificación de Información y Servicios Relacionados ECIBCE, como Autoridad de Certificación, (AC o CA por sus siglas en inglés Certification Authority) es una entidad de confianza, responsable de emitir y revocar los certificados digitales, utilizados en la firma electrónica, para lo cual se emplea la infraestructura de clave pública y servicios relacionados.

La ECIBCE posee una infraestructura de clave pública PKI (Public-Key-Infraestructure), que permite soportar la entrega de los servicios como Entidad de Certificación.

Detalle técnico de la infraestructura de clave pública.

Infraestructura de Clave Pública que sus siglas en inglés son PKI (Public Key Infraestructure) es una combinación de hardware y software, políticas y procedimientos de seguridad que permiten la ejecución de operaciones criptográficas garantizando la integridad, confidencialidad, no repudio y autenticidad de las transacciones electrónicas.

La tecnología PKI permite a los usuarios autenticarse frente a otros usuarios y usar la información de los certificados digitales (por ejemplo, las claves públicas de otros usuarios) para cifrar y descifrar mensajes, firmar electrónicamente información, permitir el uso en el doble factor de autenticación entre otros usos.

El término PKI se utiliza para referirse tanto a la Autoridad de Certificación y al resto de componentes.

La Autoridad de Certificación (o, en inglés, CA, Certificate Authority): es la encargada de emitir y revocar certificados. Es la entidad de confianza que da legitimidad a la relación de una clave pública con la identidad de un usuario o servicio.

La autoridad de registro (o, en inglés, RA, Registration Authority): es la responsable de recibir, validar, verificar y gestionar las solicitudes de emisión, revocación y renovación de certificados digitales de firma electrónica y otros servicios relacionados.

Los repositorios son las estructuras encargadas de almacenar la información relativa a la PKI. Los dos repositorios más importantes son el repositorio de certificados y el repositorio de listas de revocación de certificados– CRL, donde se incluyen todos aquellos certificados que por algún motivo han dejado de ser válidos antes de la fecha establecida dentro del mismo certificado.

La arquitectura tecnológica tiene las siguientes características generales:

- Esquema de alta disponibilidad en el Centro de Cómputo principal ubicado en el Datacenter en la ciudad de Sangolquí.
- Esquema de recuperación de desastres en caso de presentarse una contingencia, considerando como sitio alterno al Centro de Cómputo ubicado en la Dirección Zonal Guayaquil en el edificio de la Corporación Financiera Nacional.
- Los componentes asociados están instalados en las áreas exclusivas y restringidas dentro de los Centros de Cómputo principal y alterno para alojar todos los componentes de la infraestructura tecnológica.
- Esquema de seguridad en capas con el fin de proteger todos los activos de información asociados a los servicios que presta la Entidad de Certificación de Información.

- Las soluciones tecnológicas para la implementación de los servicios relacionados son especializadas y requieren cumplir con estándares internacionales de seguridad y calidad que garantice la confidencialidad, integridad y disponibilidad de la información.

6. PROCEDIMIENTO PARA GARANTIZAR PROTECCIÓN DE LOS USUARIOS.

La Entidad de Certificación de la Información del Banco Central del Ecuador (ECIBCE) cuenta con un esquema de seguridad basado en parámetros de operación y seguridad, dentro de los componentes relacionados con entornos de seguridad que se desarrollaron se destacan los siguientes: Protección llave privada, Entorno seguro, Controles físicos, Controles técnicos, Políticas de seguridad, alineación con las Normas Técnicas ISO 21188, ISO 27001 y Webtrust.

En el año 2014 la ECIBCE ejecutó una consultoría para la evaluación de cumplimiento de estándares de WebTrust en la que se identificó brechas y acciones de mejora para contar con un modelo de gestión seguro y eficiente.

El estándar WebTrust 2.0 está conformado por siete principios que corresponden a los atributos que la AC debe cumplir para poder cumplir los requerimientos del estándar. A su vez los principios se amplían en 36 criterios, que sirven como benchmark para medir objetivamente el cumplimiento de cada principio. Finalmente el estándar contempla 388 controles ilustrativos distribuidos y que corresponden a los controles sugeridos para mitigar los riesgos asociados a cada principio y criterio; estos controles son referenciales y su implementación es flexible dependiendo el contexto de la AC.

Mecanismos de seguridad de la ECIBCE

La infraestructura de Clave Pública que sus siglas en ingles son PKI (Public Key Infrastructure), se define como la arquitectura macro de la solución de Certificación Digital, el concepto de infraestructura PKI se aclara de mejor forma a través de los conceptos subyacentes:

- Seguridad a través de criptografía,
- Certificados digitales y
- Autoridad de Certificación.

Seguridad a través de la criptografía

Para mantener los datos seguros, y para proporcionarle al usuario una firma digital, cada usuario tiene varias claves diferentes. Las claves que mantienen seguros los datos son el par de claves de cifrado, que se utiliza junto con las claves simétricas. Las claves que proporcionan una firma digital se conocen como el par de claves de firma.

Seguridad de datos utilizando el par de claves de cifrado y claves simétricas

El par de claves de cifrado, utilizado junto con claves simétricas, mantiene los datos seguros. El par de claves de cifrado consiste en una clave pública (utilizada solo para "bloqueo", es decir, encriptación-datos, conocida como clave pública de encriptación) y una clave privada (utilizada solo para "desbloquear", es decir, descifrar-datos, conocida como la clave privada de descifrado). El cifrado y descifrado de datos mediante el uso de un par de claves de cifrado público-privadas se conoce como criptografía asimétrica, o, como se lo conoce más popularmente, criptografía de clave pública.

Firmas digitales utilizando el par de claves de firma digital

El par de claves de firma digital proporciona al usuario los medios para generar una firma digital. Una firma digital proporciona una garantía a un destinatario de que los datos

firmados vinieron de la persona que lo firmó, y que no se alteraron desde que se firmó. El par de claves de firma digital está compuesto por una clave de firma (conocida como la clave privada de firma) y una clave de verificación (conocida como clave pública de verificación).

Certificado Digital

Documento electrónico que contiene datos identificativos de una persona o entidad, validado por la AC del Banco Central del Ecuador, y que sirve para garantizar la identidad del autor de un mensaje o transacción electrónica.

El certificado digital como lo conocemos es simplemente un contenedor de información del par de llaves tanto públicas como privadas

Entidad de Certificación

El Banco Central del Ecuador es una entidad confiable cuya responsabilidad es certificar la autenticidad de los usuarios, por lo tanto, a través de la confianza de terceros, cualquier persona que confíe en la Autoridad de Certificación también puede confiar en la llaves del usuario, el detalle de las funciones que realiza la ECI está plasmado en la Declaración de Prácticas de Certificación (DPC) y las políticas relacionadas (PC). En la actualidad la ECI tiene los siguientes esquemas:

- Autoridad de Certificación Raíz
- Autoridad de Certificación Subordinada
- Autoridad de Registro
- Autoridad de Sellado de Tiempo

La jerarquía establecida por la ECI se basa en la Infraestructura de Clave Pública donde se establece: una AC Raíz auto firmada, una AC subordinada, autoridades de registro (AR) y los usuarios finales, que en la actualidad pueden ser del tipo: personas naturales y personas jurídicas (el tipo funcionarios públicos se extinguió en el año 2015). Los certificados que emite la ECI son multipropósito y se pueden entregar en contenedores como: token, HSM, archivo, roaming y próximamente en contenedor celular., en el caso del certificado SSL tiene como función seguridad entre sockets, y es utilizado para asegurar que los datos viajen de manera íntegra y segura, es decir, la transmisión de los datos entre un servidor y usuario web, y en retroalimentación, es totalmente cifrada o encriptada.

Lo que finalmente le hace potente a la administración de Clave Pública de la ECIBCE es el uso de dos algoritmos fundamentales en criptografía y seguridad, el RSA y el SHA. Las claves de la AC Raíz y AC Subordinada del Banco Central del Ecuador son claves RSA de 4096 bits de longitud. La generación de la función resumen (Hash) se realiza utilizando el algoritmo SHA2 de 256 bits, a continuación se describe el funcionamiento del algoritmo RSA y Algoritmo SHA 256:

Algoritmo RSA

La seguridad de este algoritmo radica en el problema de la factorización de números enteros. Los mensajes enviados se representan mediante números, y el funcionamiento se basa en el producto, conocido, de dos números primos grandes elegidos al azar y mantenidos en secreto.

Como en todo sistema de clave pública, cada usuario posee dos claves de cifrado: una pública y otra privada. Cuando se quiere enviar un mensaje, el emisor busca la clave pública del receptor, cifra su mensaje con esa clave, y una vez que el mensaje cifrado llega al receptor, este se ocupa de descifrarlo usando su clave privada.

La Infraestructura de Clave Pública - PKI se basa en dos claves, una pública y una privada. La pública, usada para cifrar, era conocida por todos; pero solamente el poseedor de la clave privada podría descifrar el mensaje.

Algoritmo SHA 256

Un algoritmo de encriptación (o cifrado) tradicional es una función que transforma un mensaje en una serie ilegible aparentemente aleatoria, usando una llave de encriptación que puede ser revertida (es decir, obtener el mensaje original) sólo por quienes conocen dicha llave. Por medio de la encriptación, la información privada puede ser enviada públicamente por internet sin mayor riesgo de que otros puedan tener acceso a ella.

SHA es una de las muchas funciones hash, una función hash es como una firma para un texto o archivo. SHA-256 es un hash de 64 dígitos hexadecimales casi único de un tamaño fijo de 256 bits (32 bytes). Un hash solo se calcula en una dirección y no se puede decodificar de vuelta.

SHA-2 se utiliza en un gran número de herramientas de seguridad y protocolos. Algunos de ellos son TLS, SSL, PGP, SSH, S/MIME, IPsec y Bitcoin.

En este sentido, la Infraestructura de Clave Pública del Banco Central del Ecuador ha adoptado los siguientes estándares tecnológicos:

- Formato de los certificados y de las listas de certificados revocados: ITU–T X509.
- Generación de las claves: RSA
- Protección de las claves privadas de certificadores y suscriptores: FIPS 140-2.

Además las siguientes Normas, Estándares y RFC referenciados para la elaboración de la DPC:

- RFC 3647: "Internet X.509 Public Key Infrastructure. Certificate Policy and Certification Practices Framework".
- RFC 3739 "Internet X.509 Public Key Infrastructure Qualified Certificates Profile".
- RFC 3280 "Internet X.509 Public Key Infrastructure Certificate and CRL Profile".
- ISO-21188:2007 "Infraestructura de llave pública para servicios financieros — Estructura de prácticas y políticas.
- RFC2560 "X.509 Internet Public Key Infrastructure Online Certificate Status Protocol OCSP".
- RFC 3161: "Internet X.509 Public Key Infrastructure. Time-Stamp Protocol (TSP)".
- RFC 3628: "Policy Requirements for Time-Stamping Authorities (TSAs)".

Contenedores criptográficos

Actualmente el certificado de firma electrónica para personas naturales y jurídicas puede ser emitido en los siguientes contendedores: archivo digital (p12), dispositivo TOKEN, dispositivo criptográfico de seguridad HSM, en dispositivo móvil tipo Smartphone o en los servidores de la ECI si se trata de uno tipo roaming.

Los certificados emitidos por la ECIBCE serán almacenados en un dispositivo criptográfico (TOKEN – SMARTCARD) en formato PKCS#11, en dispositivo criptográfico – HSM en formato PKCS#10, en Dispositivos Móviles (IOS y Android) en formato PKCS#11, en archivo digital en formato PKCS#12 (PFX o P12) o servidor roaming para usuarios finales, y certificados de servidor seguro o web en formato PKCS#10, de acuerdo a las políticas de certificados, manteniendo niveles y estándares de seguridad.

Los certificados de usuario final emitidos en TOKEN, Archivo y Roaming pueden tener hasta 2 pares de claves, es decir, de "Firma Digital" y "Cifrado", cada uno con la clave pública y clave privada; por otra parte los emitidos en Dispositivos Móviles (IOS y Android) pueden

tener hasta 3 pares de claves: de "Firma Digital", de "Autenticación" y de "Cifrado", mientras que los certificados emitidos en un HSM solo tiene 1 par de claves para "Firma Digital".

Los certificados emitidos en dispositivos criptográficos, deberán ser los reconocidos por la ECIBCE, los mismos que deben cumplir con los mínimos niveles de seguridad como FIPS 1 nivel 2 o superior. Los dispositivos criptográficos aceptados por la ECIBCE y sus AR serán publicados en la página web de la ECIBCE.

Los dispositivos serán entregados de manera personal al suscriptor por parte de la AR de la ECIBCE. En cuanto a los dispositivos móviles (IOS y Android), su propiedad, procedencia y titularidad es de exclusiva responsabilidad del solicitante de firma electrónica.

En el caso particular de los token es pertinente indicar que el certificado se guarda de forma segura ya que cumple con las normas de seguridad FIPS (Federal Information Processing Standard), avalados por el NITS (Instituto Nacional de Normas y Tecnología - National Institute of Standards and Technology). Estas normas son estándares de seguridad del Gobierno Estadounidense para el procesamiento de la información, y que fueron adoptadas por la ECI para elevar los niveles de seguridad en el uso de sus certificados en especial de los dispositivos TOKEN. La seguridad cubre: a nivel externo sus componentes, a nivel interno, su chip criptográfico; lo que garantiza que el dispositivo no sea vulnerable en ninguna de sus partes y que la información contenida esté criptográficamente custodiada.

Especificaciones técnicas de los tokens

Los Token utilizados por el BCE ofrecen autentificación de dos factores para el acceso seguro remoto y de red, además de compatibilidad basada en certificados con aplicaciones de seguridad avanzadas, incluidas la firma digital y la autentificación previa al inicio.

La última adquisición de tokens es el modelo SafeNet eToken 5110 se basa en la avanzada plataforma IDCore de Gemalto y se integra sin dificultad con aplicaciones externas mediante las herramientas de desarrollo de SafeNet Authentication, es compatible con aplicaciones de gestión SafeNet PKI (infraestructura de clave pública) y contraseñas, así como herramientas de desarrollo de software.

Además, permite la personalización de las aplicaciones y la ampliación de las funciones mediante applets de Java integrados. Así mismo, SafeNet eToken 5110 es compatible con SafeNet Authentication Manager, lo cual reduce los gastos generales de TI al optimizar todas las operaciones de autentificación como la implementación, la provisión, la inscripción y el mantenimiento continuo. SafeNet eToken 5110 también es compatible con SafeNet Authentication Client que ofrece una total administración y soporte para lograr gestión, eventos e implementación avanzados.

Estándares y normas internacionales

Para garantizar un nivel de seguridad dentro de la gestión de la plataforma PKI el Banco Central del Ecuador en calidad de entidad de Certificación de Información ha aplicado normas internacionales de seguridad emitidas y aprobadas por la ISO y la ITU.

Norma ISO/IEC 9594-8 Estándar X.509

El formato de los certificados utilizados por la ECI está definido por el estándar internacional ITU-T X.509. De esta forma, los certificados pueden ser leídos o escritos por cualquier aplicación que cumpla con el mencionado estándar.

Adoptando el estándar Internacional que establece para Certificados de Clave Pública (PKI), 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. Una CRL es un archivo firmado por la AC, que contiene la fecha de emisión de la CRL y una lista de certificados revocados, cada uno de ellos con la fecha de revocación. Una CRL puede ser verificada como cualquier otro documento firmado digitalmente, en este caso con la Infraestructura de clave Pública de la AC, al utilizar una CRL se confía en su veracidad y se determina con certeza si un certificado esta revocado o no, esto es hasta la fecha definida por última actualización.

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 2560 – X.509 Infraestructura de Clave Pública Internet. PKI Protocolo en línea del Estado del Certificado – OCSP (Online Certificate Status Protocol).

Este protocolo especifica el estado de un certificado digital, tomando como base la lista de certificados revocados (CRL) en la infraestructura PKI. 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 de 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.

La ECIBCE tiene implementado el protocolo OCSP a fin de garantizar a los usuarios la validez o revocación de los mismos de manera óptima y segura.

FIPS 140 (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.

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.

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.

El estándar mencionado propone un esquema incremental de exigencias de seguridad, basado en 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.

El BCE utiliza dispositivos criptográficos con niveles de seguridad FIPS 140-2 niveles 2 y 3, a continuación una descripción:

- 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 140–3 nivel 3: además de los mecanismos de seguridad física evidentes a prueba de manipulaciones requeridos en el Nivel de seguridad 2, el Nivel de seguridad 3 incluye intentos para evitar que el intruso obtenga acceso a los Proveedores de Servicios Criptográficos - CSP que se encuentran dentro del módulo criptográfico.

  Los mecanismos de seguridad física requeridos en el Nivel de Seguridad 3 tienen la intención de tener una alta probabilidad de detectar y responder a intentos de acceso físico, uso o modificación del módulo criptográfico.

  Los mecanismos de seguridad física pueden incluir el uso de cerramientos fuertes y detección / respuesta de manipulación circuitería que pone a cero todos los CSP de texto sin formato cuando las cubiertas / puertas extraíbles del módulo criptográfico son abiertos.

  El Nivel 3 de seguridad requiere mecanismos de autenticación basados en la identidad, mejorando la seguridad brindada por el mecanismo de autenticación basado en roles especificados para el Nivel de seguridad 2.

  Un módulo criptográfico autentica la identidad de un operador y verifica que el operador identificado está autorizado a asumir una función específica y realizar un conjunto correspondiente de servicios.

  El Nivel de seguridad 3 requiere la entrada o salida de CSP de texto simple (incluida la entrada o salida de texto sin formato) CSP que utilizan los procedimientos de división de conocimiento) se realizan utilizando puertos que están físicamente separados de otros puertos, o interfaces que están separados lógicamente utilizando una ruta de confianza de otras interfaces.

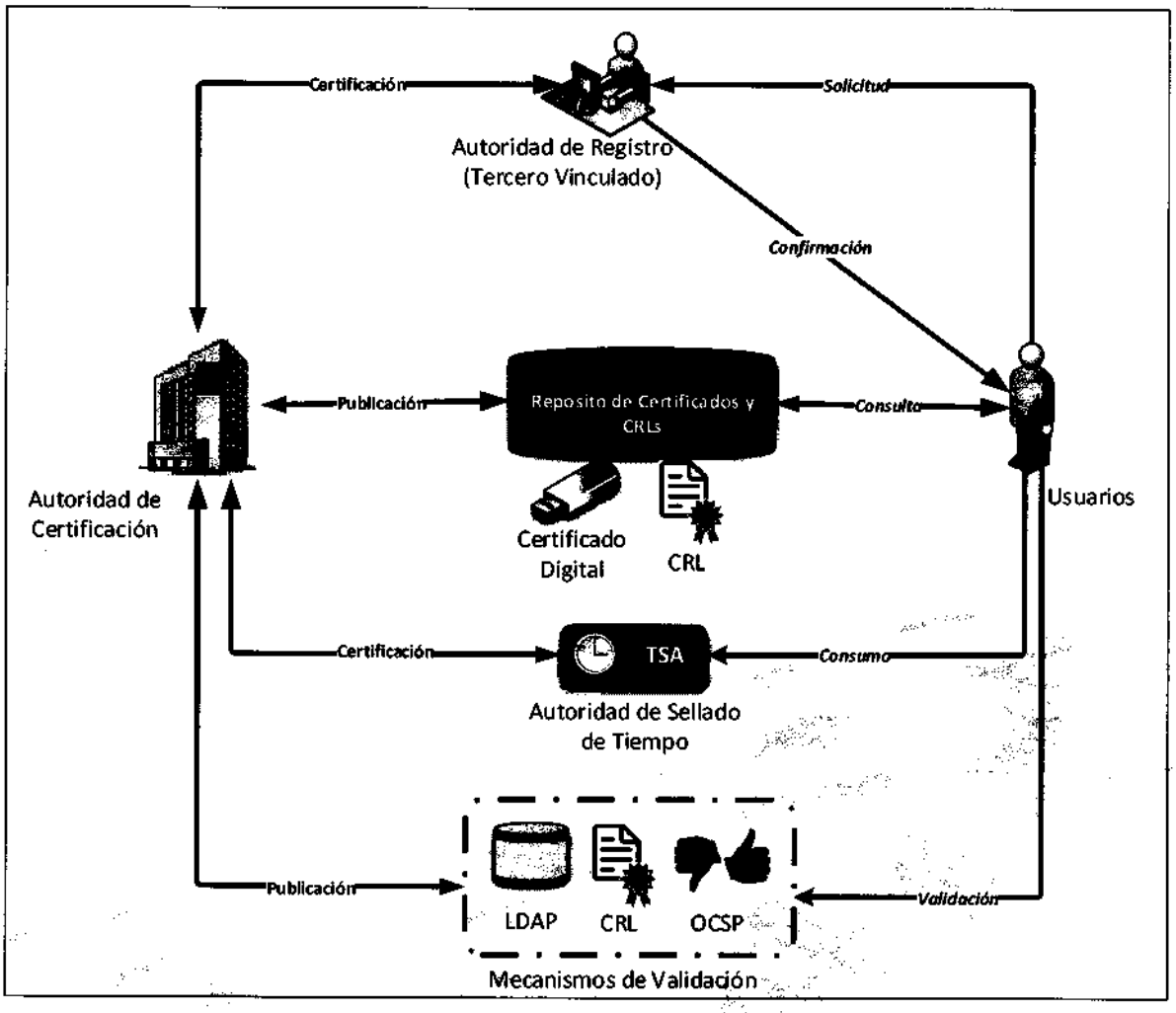
  La autenticación (y otros servicios de seguridad) solo se pueden proporcionar dentro del contexto de una política de seguridad definida. Es una cuestión para los usuarios de una aplicación definir su propia política de seguridad.

  En este contexto la ECI ante la adopción de estándares tecnológicos internacionalmente aceptados garantiza que frente a cualquier transacción que involucre el uso de un certificado digital, permite asegurar un proceso efectivo de verificación de dichas firmas, otorgando seguridad técnica y legal a las transacciones electrónicas en el país.

7. ÁREA DE COBERTURA:

Nivel Nacional.

8. DIAGRAMA ESQUEMÁTICO INFRAESTRUCTURA DE PKI.



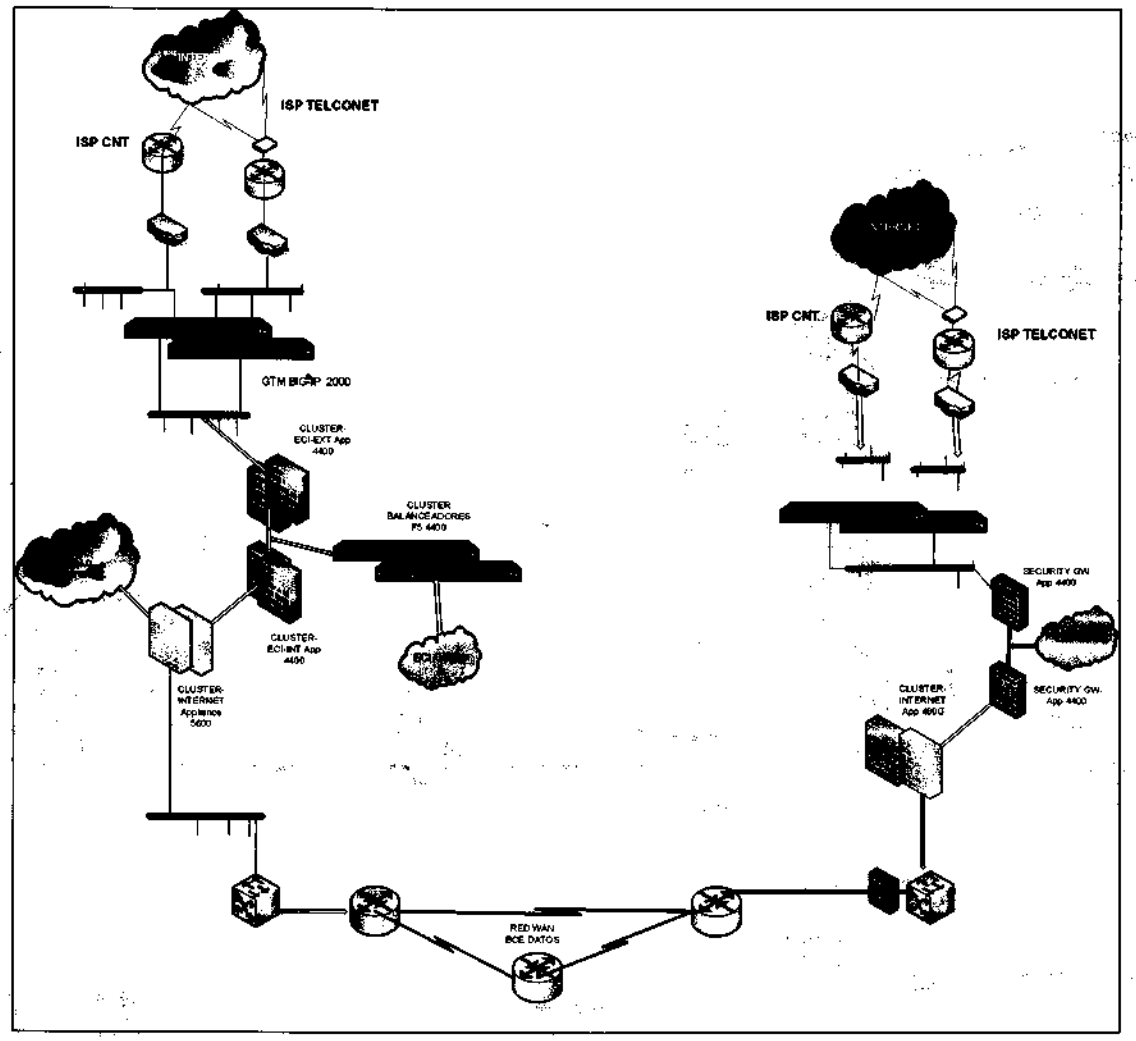
Los componentes tecnológicos de la infraestructura PKI del Banco Central del Ecuador son los siguientes:

Componente	Aplicación	Plataforma
Autoridad de Certificación (AC)	Entrust Authority Security Manager	Red Hat Enterprise Linux 5.4
Autoridad de Certificación Subordinada	Entrust Authority Security Manager	Microsoft Windows Server 2008 R2
Repositorio de Certificados Digitales (LDAP RAIZ)	Open Ldap	Red Hat Enterprise Linux 6.0
Repositorio de Certificados Digitales (LDAP Subordinado)	Open Ldap	Red Hat Enterprise Linux 6.0
Administration Services	Entrust Authority™ Administration	Microsoft Windows Server 2008 R2
Lista de Certificados Revocados	Apache	Red Hat Enterprise Linux 6
Protocolo de comprobación del Estado de un Certificado	OCSP-EJBCA	Red Hat Enterprise Linux 5.5

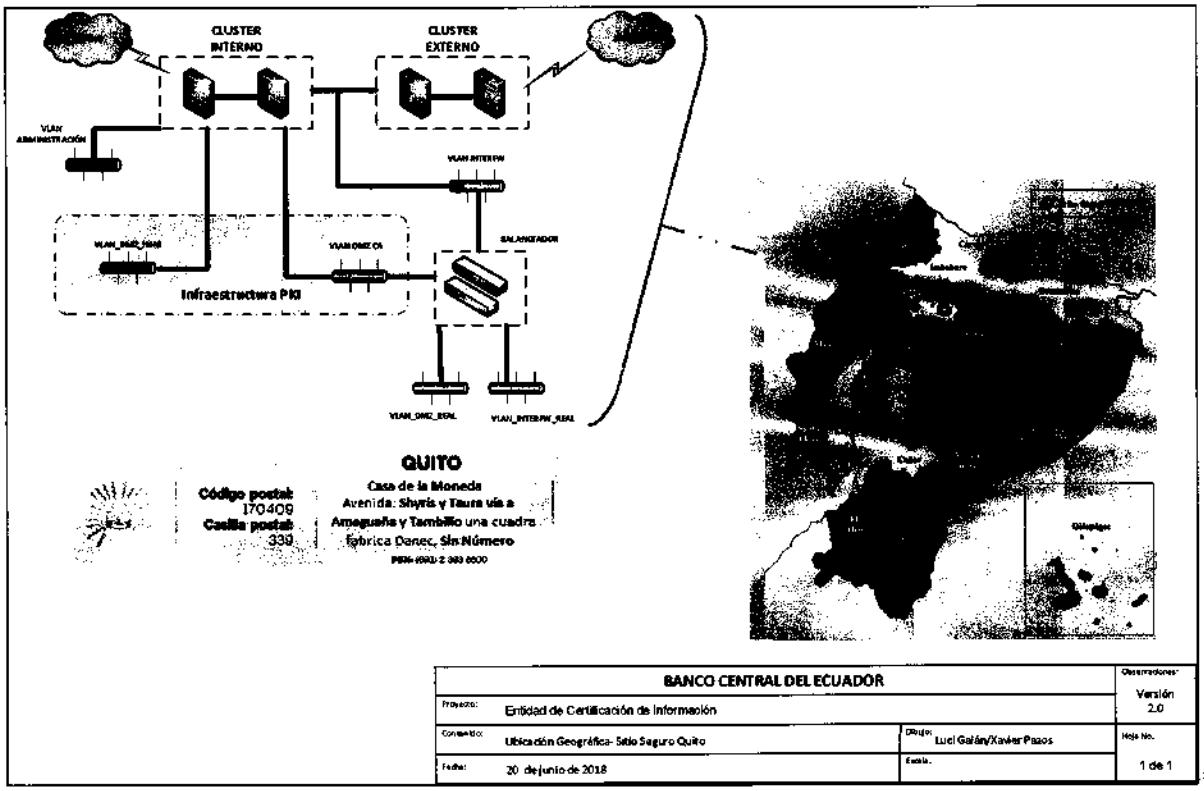
Componente	Aplicación	Plataforma
En línea (OCSP)		
Protocolo de comprobación del Estado de un Certificado En línea (OCSP)	KeyOne Validation Authority	Microsoft Windows Server 2012 R2 Standar
Contenedor Certificado Roaming	Entrust Authority™ Roaming Server	Microsoft Windows Enterprise 2008
Contenedor Certificado Archivo	Entrust Authority™ Digital Identity Manager	Microsoft Windows Server 2008 R2 Enterprise
Contenedor Certificado Token	Api Generación Certificados en contenedor Token	Solaris 10
Sellado de Tiempo	Ascertia	Microsoft Windows Server 2012 R2 Standar

Adicionalmente, y con el fin de garantizar la disponibilidad de los servicios asociados a la infraestructura PKI, el Banco Central del Ecuador dispone de una arquitectura de alta disponibilidad y desarrolló un plan de contingencia, considerando como sitio alterno a la Dirección Zonal Guayaquil.

9. ESQUEMA DE SEGURIDAD PERIMETRAL



10. SITIOS SEGUROS



11. CUMPLIMIENTO DE OBLIGACIONES CONTRACTUALES

Con base a los informe técnicos: IT-CZ05-C-2018-0548 e IT-CZ02-C-2018-0946, emitidos por las Coordinaciones Zonales 05 y 02, así como al informe técnico IT-CCDS-RS-2018-183 de la Dirección de Control de Servicios de Telecomunicaciones, se determinó que la ECIBCE, se encuentra operando conforme a su acreditación y a las adecuaciones y modificaciones de infraestructura registradas en la Agencia de Regulación y Control de las Telecomunicaciones.

12. INFORMACIÓN INCLUIDA EN SOLICITUD

El solicitante adjunta en su solicitud lo siguiente:

- Copia de la cédula de ciudadanía de la representante legal del Banco Central del Ecuador.
- Copia del certificado de votación del último proceso eleccionario.
- Proyecto de Renovación de la Acreditación de la Entidad de Certificación de la Información del Banco Central del Ecuador.
- Diagrama esquemático y descripción técnica detallada de la infraestructura.
- Descripción detallada de cada servicio propuesto y de los recursos e infraestructura disponibles.
- Portafolio de servicios / Productos de la Entidad de Certificación de la Información del Banco Central del Ecuador (ECIBCE).
- Diagrama técnico detallado de cada "Nodo" o "Sitio Seguro" y especificaciones técnicas de los equipos.
- Documentos de soporte que confirmen que se dispone de mecanismos de seguridad.
- Ubicación geográfica de cada nodo o sitio seguro.
- Anexo A Declaración de Prácticas de Certificación – DPC.
- Anexo B1 Políticas de Certificado de Firma Electrónica de Persona Natural.

- Anexo B2 Políticas de Certificado de Firma Electrónica de Persona Jurídica.
- Anexo C Declaración de Prácticas de Certificación de sellado de tiempo.
- Anexo D Contrato de Tercero Vinculado.
- Anexo E Ley de Comercio Electrónico, Firmas y Mensajes de Datos.
- Anexo F Esquema Gubernamental de seguridad de la información EGSI.
- Anexo G Especificaciones Tokens.
- Anexo H Plan de Contingencias.
- Anexo I Especificaciones técnicas Hardware.
- Copia de la Certificación Ordinaria Nro. CO – 780 de 2 de julio de 2018 por USD 22,000.00.
- Copia de la Constancia Nro. 0003788 de 2 de julio de 2018.
- Copia de la Póliza de Seguro de Responsabilidad Civil Nro. 10001085 emitida por Seguros Sucre con una suma asegurada de USD 400,000.00 con una vigencia desde el 31/12/2017 hasta el 31/12/2019.

13. DURACIÓN DE LA ACREDITACIÓN

Conforme al Decreto Ejecutivo No. 1356 "*Reformas al Reglamento General a la Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos. Art. 4.- (…)*
El plazo de duración de la acreditación será de 10 años renovables por igual período, previa solicitud escrita…"

14. DERECHOS DE LA ACREDITACIÓN

Conforme al Decreto Ejecutivo No. 1356 "*Reformas al Reglamento General a la Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos. "La acreditación como Entidad de Certificación de Información y Servicios Relacionados comprende el derecho para la instalación, modificación ampliación y operación de la infraestructura requerida para tal fin y estará sujeta al pago de valores, los que serán fijados por el CONATEL.*"

15. CONCLUSIONES.

- La Entidad de Certificación de Información y Servicios Relacionados del Banco Central del Ecuador, ha cumplido con las obligaciones contractuales y normativas establecidas en la Acreditación otorgada conforme lo establece la Ley de Comercio Electrónico, por lo que técnicamente sería factible renovar la Acreditación de Entidad de Certificación de Información y Servicios Relacionados a favor del Banco Central del Ecuador.

SECCIÓN II

INFORME ECONÓMICO - FINANCIERO

INFORME ECONÓMICO – FINANCIERO

I. ANTECEDENTES DE LA INSTITUCIÓN

El Banco Central del Ecuador es una Entidad de Certificación de Información y Servicios Relacionados (ECIBCE) acreditada por el ex Consejo Nacional de Telecomunicaciones, mediante Resolución 481-20-CONATEL-2008 de 8 de octubre de 2008 y acto administrativo suscrito el 6 de noviembre de 2008.
La misma tiene la misión de Emitir certificados digitales de firma electrónica y otros servicios relacionados con la certificación electrónica para Personas Jurídicas y Personas Naturales; garantizando la seguridad jurídica y tecnológica en entornos electrónicos cumpliendo el marco legal, las normas y estándares nacionales e internacionales de certificación electrónica.
La ECIBCE posee una infraestructura de clave pública PKI (Public-Key-Infraestructure), que permite soportar la entrega de los servicios como Entidad de Certificación.
De acuerdo a los Informes de Rendición de Cuentas del Banco Central del Ecuador se han emitido en el 2016 y 2017 un total de 76,680 certificaciones para ser utilizadas en las siguientes aplicaciones:

- Sistema de Gestión Documental QUIPUX
- Sistema Nacional de Pagos (BCE)
- Cámara de Compensación de Cheques (BCE)
- Servicio Nacional de Aduana (SENAE)
- Facturación Electrónica (SRI)
- Sistema de Contratación Pública del SERCOP
- Sistema de Registro de Datos Vitales (REVIT) - Ministerio de Salud
- Balances Electrónicos - Superintendencia de Compañías

Estas certificaciones han permitido simplificar y optimizar la atención a trámites de usuarios del sector público, privado y ciudadanía en general. Esto demuestra la importancia de la renovación de la acreditación del Banco Central del Ecuador como Entidad de Certificación de Información y Servicios Relacionados.

II. ANÁLISIS DE CAPACIDAD ECONÓMICA Y FINANCIERA

Mediante Oficio Nro. BCE-BCE-2018-0465-OF de 06 de julio de 2018, ingresado mediante trámite Nro. ARCOTEL-CTDS-2018-0009-E de 06 de julio de 2018, el Banco Central del Ecuador en cumplimiento al artículo cuatro, literal *"l)"* del Decreto N° 1356 para las Reformas al Reglamento General a la Ley de comercio electrónico, firmas electrónicas y mensajes de datos de fecha 29 de septiembre de 2008, el cual establece los requisitos del peticionario de una acreditación como Entidad de Certificación de Información y Servicios Relacionados, debería presentar los siguientes documentos: *"(...) l) Información que demuestre la capacidad económica y financiera para la prestación de servicios de certificación de información y servicios relacionados (...)"*; presentó los siguientes documentos:

- Copia de la Certificación Ordinaria Nro. CO – 780 de 2 de julio de 2018 por USD 22,000.00
- Copia de la Constancia Nro. 0003788 de 2 de julio de 2018 por USD 22,000.00
- Copia de la Póliza de Seguro de Responsabilidad Civil Nro. 10001085 emitida por Seguros Sucre con una suma asegurada de USD 400,000.00 con una vigencia desde el 31/12/2017 hasta el 31/12/2019.

De acuerdo al Código Orgánico, Monetario y Financiero, El Banco Central del Ecuador es una persona jurídica de derecho público, parte de la Función Ejecutiva, de duración indefinida, con autonomía administrativa y presupuestaria.
Su presupuesto se financiará con los ingresos obtenidos por su propia gestión y se elaborará en base a los lineamientos que emita la Junta de Política y Regulación Monetaria y Financiera y demás leyes relacionadas con la materia.

En este sentido la ECIBCE ha venido funcionando con normalidad ya que anualmente se asignan los recursos económicos necesarios para continuar sus operaciones, tal es el caso de la asignación de los valores que deben ser cancelados para la renovación de su acreditación como Entidad de Certificación de Información y Servicios Relacionados:

BANCO CENTRAL DEL ECUADOR

SISTEMA DE PRESUPUESTO

CERTIFICACION ORDINARIA

QUITO **CO- 780**

Por: 22,000.00 Dólares

El Director o su Delegado del CRP: DIRECCIÓN NACIONAL DE SERVICIOS FINANCIEROS - C en atención al SEGÚN CORREO DEL 26/06/2018 EN EL CUAL SOLICITA JUAN JOSE DARQUEA LA CERTIFICACIÓN DE FONDOS COMO REQUISITO PARA PRESENTAR EN ARCOTEL COMO PARTE DEL PROCEDO DE RENOVACIÓN DE LA ACREDITACION DE ECE ha verificado la documentación del

CERTIFICA QUE:

En la partida presupuestaria:

Cuenta : 412205

Auxiliar : 40079500000000 OTROS SERV.ESPECIALIZADOS CENTRALIZADO

Detalle : 0 OTROS SERV.ESPECIALIZADOS CENTRALIZADOS QUITO

CRP : 5042 DIRECCIÓN NACIONAL DE SERVICIOS FINANCIEROS - C

RENOVACIÓN DE LA ACREDITACIÓN ANTE EL ARCOTEL, DE LA ENTIDAD DE CERTIFICACIÓN DE INFORMACIÓN DEL BANCO CENTRAL DEL ECUADOR

QUITO, 2 de Julio de 2018

82442 - SANTILLAN COELLO ANDREA MIREYA

Banco Central del Ecuador

CONSTANCIA - 0003788

Fecha: 02/07/2018 09:03:58
Actividad: 2916 - RENOVACIÓN DE LA ACREDITACIÓN ANTE EL ARCOTEL, DE LA ENTIDAD DE CERTIFICACIÓN DE INFORMACIÓN DEL BANCO CENTRAL DEL ECUADOR
Observación: RENOVACIÓN DE LA ACREDITACIÓN DE LA ENTIDAD DE CERTIFICACIÓN ELECTRÓNICA
CRP: 5042
Cuenta: 412205
Auxiliar: 40079500000000
Partida: OTROS SERV.ESPECIALIZADOS CENTRALIZADOS QUITO
Detalle: 0 - OTROS SERV.ESPECIALIZADOS CENTRALIZADOS QUITO

Valor 2018: $	22,000
Total Constancia: $	22,000

SANTILLAN COFLAO ANDREA MIREYA

SegurosSucre
La certeza de un futuro tranquilo

Seguros Sucre S.A en adelante "la Compañía" y quien(es) más adelante se denomina(n) con el nombre del "Asegurado", convienen en celebrar el presente contrato de seguro, sujeto a las condiciones generales aprobadas por la Superintendencia de Bancos mediante Resolución N° SB-INJ-2001-216 16 de AGOSTO del 2001 y particulares y especiales, teniendo prelación las últimas sobre las primeras. RUC.: 0190151174001

SEGURO DE: RESPONSABILIDAD CIVIL	PÓLIZA N° 10001085	VIGENCIA
MONEDA: DÓLAR DE LOS ESTADOS UNIDOS DE AMÉRICA	ANEXO N° 00000000	Desde el:31/12/2017 a las12h00 Hasta el:31/12/2019 a las12h00
SUMA ASEGURADA: USD 400,000.00		Plazo: 730 días

ASEGURADO: BANCO CENTRAL DEL ECUADOR(S)
AV. 10 DE AGOSTO N 11-409 Y ARICENO - QUITO, ECUADOR CENTRO TEL.: 023958600
PICHINCHA-QUITO

OBJETO ASEGURADO O CAUSA DE LA MODIFICACIÓN:
SEGUN CONDICIONES GENERALES Y PARTICULARES ADJUNTAS.

Cláusulas que forman parte de este contrato:
SEGUN CONDICIONES PARTICULARES
PROBALINO
Forma de pago:
C O N T A D O

PRIMA NETA USD 30,000.00	CONSTANCIA(S,DIS) 1,050.00
S. SOCIAL CAMPESINO(0.50%) 150.00	DERECHO DE EMISION 9.00
SUBTOTAL TARIFA IVA(0.00%) 0.00	SUBTOTAL TARIFA IVA(12.00%) 31,209.00
I.V.A(12.00%) 3,745.00	(-) COMISIONES ESTIMADAS(0.0 0.00
INTERESES 0.00	TOTAL 34,954.00

En testimonio de lo acordado se firma este contrato en: QUITO D.M., 1 DE FEBRERO DE 2018

EL ASEGURADO

SEGUROS SUCRE S.A.

FIRMA AUTORIZADA

III. OBLIGACIONES ECONÓMICAS

Mediante Memorando Nro. ARCOTEL-CTDG-2018-0530-M de 02 de octubre de 2018, el Mgs. Marco Logacho, Director Técnico de Gestión Económica de Títulos Habilitantes, informa: *"Una vez analizada la información proporcionada por la Coordinación Administrativa Financiera, mediante memorando Nro. ARCOTEL-CAFI-2018-0683-M de 25 de septiembre de 2018, así como el registro histórico de pagos obtenido del SIFAF (impresión de pantalla), adjunto al memorando indicado; se concluye que el BANCO CENTRAL DEL ECUADOR no mantiene obligaciones pendientes de pago con la ARCOTEL. Cabe señalar, que con oficio Nro. BCE-DNSF-2018-0702-OF de 27 de septiembre de 2018 el Director Nacional de Servicios Financieros del Banco Central del Ecuador, presenta una póliza de Responsabilidad Civil con vigencia hasta el 31 de diciembre de 2019."*

IV. CONCLUSION

El Banco Central del Ecuador ha cumplido hasta la fecha con sus obligaciones económicas con la ARCOTEL y demuestra que tiene la capacidad económica y financiera para continuar con la prestación de servicios de certificación de información y servicios relacionados.

SECCIÓN III

INFORME JURÍDICO

INFORME JURÍDICO

1. CONSIDERACIONES JURÍDICAS:

La Constitución de la República del Ecuador, señala:

"Art. 16.- *Todas las personas, en forma individual o colectiva, tienen derecho a: 3. La creación de medios de comunicación social, y al acceso en igualdad de condiciones al uso de las frecuencias del espectro radioeléctrico para la gestión de estaciones de radio y televisión públicas, privadas y comunitarias, y a bandas libres para la explotación de redes inalámbricas".*

*"**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".*

***"Art. 261.-** El Estado central tendrá competencias exclusivas sobre: 10. El espectro radioeléctrico y el régimen general de comunicaciones y telecomunicaciones; puertos y aeropuerto (...)".*

*"**Art. 313.-** El Estado se reserva el derecho de administrar, regular, controlar y gestionar los sectores estratégicos, de conformidad con los principios de sostenibilidad ambiental, precaución, prevención y eficiencia.- Los sectores estratégicos, de decisión y control exclusivo del Estado, son aquellos que por su trascendencia y magnitud tienen decisiva influencia económica, social, política o ambiental, y deberán orientarse al pleno desarrollo de los derechos y al interés social.- Se consideran sectores estratégicos la energía en todas sus formas, las telecomunicaciones, los recursos naturales no renovables, el transporte y la refinación de hidrocarburos, la biodiversidad y el patrimonio genético, el espectro radioeléctrico, el agua, y los demás que determine la ley".*

***"Art. 314.-** El Estado será responsable de la provisión de los servicios públicos de agua potable y de riego, saneamiento, energía eléctrica, telecomunicaciones, vialidad, infraestructuras portuarias y aeroportuarias, y los demás que determine la ley.*

El Estado garantizará que los servicios públicos y su provisión respondan a los principios de obligatoriedad, generalidad, uniformidad, eficiencia, responsabilidad, universalidad, accesibilidad, regularidad, continuidad y calidad. El Estado dispondrá que los precios y tarifas de los servicios públicos sean equitativos, y establecerá su control y regulación."

La Ley Orgánica de Telecomunicaciones, señala:

***"Art. 144.-** Competencias de la Agencia. "29. Regular y controlar las actividades relacionadas con el comercio electrónico y firma electrónica, de conformidad con el ordenamiento jurídico vigente.".*

Disposiciones Derogatorias

***"Primera.-** Se suprime la Superintendencia de Telecomunicaciones, el Consejo Nacional de Telecomunicaciones (CONATEL) y la Secretaría Nacional de Telecomunicaciones. Las partidas presupuestarias, los bienes muebles e inmuebles, activos y pasivos, así como los derechos y obligaciones derivados de contratos, convenios e instrumentos nacionales e internacionales correspondientes a dichas entidades, pasan a la Agencia de Regulación y Control de las Telecomunicaciones. Los derechos y obligaciones derivados de contratos, convenios e instrumentos nacionales e internacionales relacionados con la planificación del uso del espectro radioeléctrico, así como la elaboración del Plan Nacional de Frecuencias, son asumidos por la Agencia de Regulación y Control de las Telecomunicaciones.".*

"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."*

La Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos, expresa:

*"**Art. 1.**- Objeto de la ley.- Esta ley regula los mensajes de datos, la firma electrónica, los servicios de certificación, la contratación electrónica y telemática, la prestación de servicios electrónicos, a través de redes de información, incluido el comercio electrónico y la protección a los usuarios de estos sistemas."*

"**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. 30.**- Obligaciones de las entidades de certificación de información acreditadas.- Son obligaciones de las entidades de certificación de información acreditadas:*

a) Encontrarse legalmente constituidas, y estar registradas en Consejo Nacional de Telecomunicaciones;
b) Demostrar solvencia técnica, logística y financiera para prestar servicios a sus usuarios;
c) Garantizar la prestación permanente, inmediata, confidencial, oportuna y segura del servicio de certificación de información,
d) Mantener sistemas de respaldo de la información relativa a los certificados;
e) Proceder de forma inmediata a la suspensión o revocatoria de certificados electrónicos previo mandato del Superintendente de Telecomunicaciones, en los casos que se especifiquen en esta ley;
f) Mantener una publicación del estado de los certificados electrónicos emitidos;
g) Proporcionar a los titulares de certificados de firmas electrónicas un medio efectivo y rápido para dar aviso que una firma electrónica tiene riesgo de uso indebido;
h) Contar con una garantía de responsabilidad para cubrir daños y perjuicios que se ocasionaren por el incumplimiento de las obligaciones previstas en la presente ley, y hasta por culpa leve en el desempeño de sus obligaciones. Cuando certifiquen límites sobre responsabilidades o valores económicos, esta garantía será al menos del 5% del monto total de las operaciones que garanticen sus certificados; e,
i) Las demás establecidas en esta ley y los reglamentos."

*"**Art. 31.**- Responsabilidades de las entidades de certificación de información acreditadas.- Las entidades de certificación de información serán responsables hasta de culpa leve y responderán por los daños y perjuicios que causen a cualquier persona natural o jurídica, en el ejercicio de su actividad, cuando incumplan las obligaciones que les impone esta ley o actúen con negligencia, sin perjuicio de las sanciones previstas en la Ley Orgánica de Defensa del Consumidor. Serán también responsables por el uso indebido del certificado de firma electrónica acreditado, cuando éstas no hayan consignado en dichos certificados, de forma clara, el límite de su uso y del importe de las transacciones válidas que pueda realizar. Para la aplicación de este artículo, la carga de la prueba le corresponderá a la entidad de certificación de información.*

Los contratos con los usuarios deberán incluir una cláusula de responsabilidad que reproduzca lo que señala el primer inciso.

Cuando la garantía constituida por las entidades de certificación de información acreditadas no cubra las indemnizaciones por daños y perjuicios, aquellas responderán con su patrimonio."

"***Art. 33.-*** *Prestación de servicios de certificación por parte de terceros.- Los servicios de certificación de información podrán ser proporcionados y administrados en todo o en parte por terceros. Para efectuar la prestación, éstos deberán demostrar su vinculación con la Entidad de Certificación de Información.*

El Consejo Nacional de Telecomunicaciones, establecerá los términos bajo los cuales las Entidades de Certificación de Información podrán prestar sus servicios por medio de terceros".

*"**Art. 34**.- Terminación contractual.- La terminación del contrato entre las entidades de certificación acreditadas y el suscriptor se sujetará a las normas previstas en la Ley Orgánica de Defensa del Consumidor."*

*"**Art. 37.-** 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.".

*"**Art. 38.-** Organismo de control de las entidades de certificación de información acreditadas.- Para efectos de esta ley, la Superintendencia de Telecomunicaciones, será el organismo encargado del control de las entidades de certificación de información acreditadas."*

El Reglamento General a la Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos, establece:

*"**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.".*

*"**Art. ...-** Registro Público Nacional de Entidades de Certificación de Información y Servicios Relacionados Acreditadas y terceros vinculados: "Se crea el Registro Público Nacional de Entidades de Certificación de Información y Servicios Relacionados Acreditadas y terceros vinculados, a cargo de la Secretaría Nacional de Telecomunicaciones..."*

*"**Art. ...-** Acreditación: La acreditación como Entidad de Certificación de Información y Servicios Relacionados, consistirá en un acto administrativo emitido por el CONATEL a través de una resolución la que será inscrita en el Registro Público Nacional de Entidades de Certificación de Información y Servicios Relacionados Acreditadas y terceros vinculados.*

El plazo de duración de la acreditación será de 10 años renovables por igual período, previa solicitud escrita presentada a la Secretaría Nacional de Telecomunicaciones con tres meses de anticipación al vencimiento del plazo, siempre y cuando la Entidad de Certificación de Información y Servicios Relacionados Acreditada haya cumplido con sus obligaciones legales y reglamentarias, así como las que consten en la resolución de acreditación.

La acreditación como Entidad de Certificación de Información y Servicios Relacionados comprende el derecho para la instalación, modificación ampliación y operación de la

infraestructura requerida para tal fin y estará sujeta al pago de valores, los que serán fijados por el CONATEL."

*"**Art.** ...- Requisitos para la Acreditación: El peticionario de una acreditación como Entidad de Certificación de Información y Servicios Relacionados, deberá presentar los siguientes documentos:*

a) Solicitud dirigida a la Secretaria Nacional de Telecomunicaciones, detallando nombres y apellidos completos del representante legal, dirección domiciliaria de la empresa unipersonal o compañía;

b) Copia de la cédula de ciudadanía del representante legal o pasaporte según corresponda;

c) Copia del certificado de votación del último proceso eleccionario (correspondiente al representante legal, excepto cuando se trate de ciudadanos extranjeros);

d) Copia certificada e inscrita en el Registro Mercantil (excepto las instituciones públicas) del nombramiento del representante legal;

e) Copia certificada debidamente registrada en el Registro Mercantil, de la escritura de constitución de la empresa unipersonal o compañía y reformas en caso de haberlas (excepto las instituciones públicas);

f) Original del certificado de cumplimiento de obligaciones emitido por la Superintendencia de Compañías o Bancos y Seguros según corresponda, a excepción de las instituciones del Estado;

g) Diagrama esquemático y descripción técnica detallada de la infraestructura a ser utilizada, indicando las características técnicas de la misma;

h) Descripción detallada de cada servicio propuesto y de los recursos e infraestructura disponibles para su prestación. La SENATEL podrá ordenar inspecciones o verificaciones a las instalaciones del peticionario cuando lo considere necesario;

i) Documentos de soporte que confirmen que se disponen de mecanismos de seguridad para evitar la falsificación de certificados, precautelar la integridad, resguardo de documentos, protección contra siniestros, control de acceso y confidencialidad durante la generación de claves, descripción de sistemas de seguridad, estándares de seguridad, sistemas de respaldo;

j) Ubicación geográfica inicial, especificando la dirección de cada nodo o sitio seguro;

k) Diagrama técnico detallado de cada "Nodo" o "Sitio Seguro" detallando especificaciones técnicas de los equipos;

l) Información que demuestre la capacidad económica y financiera para la prestación de servicios de certificación de información y servicios relacionados;

m) En caso de solicitud de renovación de la acreditación y de acuerdo con los procedimientos que señale el CONATEL, deberán incluirse los requisitos de carácter técnico, la certificación de cumplimiento de obligaciones por parte de la Superintendencia de Telecomunicaciones, en la que constará el detalle de imposición de sanciones, en caso de haber/as y el informe de cumplimiento de obligaciones por parte de la Secretaría Nacional de Telecomunicaciones.

*"**Art.** ...- Procedimiento de Acreditación: La solicitud acompañada de todos los requisitos establecidos será presentada ante la Secretaría Nacional de Telecomunicaciones, la que*

dentro del término de tres días procederá a publicar un extracto de la misma en su página WEB institucional.

Dentro del término de 15 días contados desde la fecha de presentación de la solicitud, la SENATEL remitirá al CONATEL los informes técnico, legal y económico-financiero en base a la documentación presentada.

El CONATEL, dentro del término de 15 días resolverá el otorgamiento de la acreditación. Copia certificada de la resolución de acreditación será remitida a la Secretaría Nacional de Telecomunicaciones dentro del término de dos días, a fin de que ésta dentro del término de cinco días, previo el pago por parte del solicitante, de los valores que el CONATEL haya establecido para el efecto, realice la inscripción en el Registro Público Nacional de Entidades de Certificación de Información y Servicios Relacionados Acreditadas y terceros vinculados y efectúe la notificación al peticionario.

En el evento de que el peticionario no cancele los valores correspondientes por la acreditación dentro del término de 15 días, el acto administrativo quedará sin efecto automáticamente y la Secretaría Nacional de Telecomunicaciones procederá al archivo del trámite."

*"**Art.** ...- Contenido mínimo de la Acreditación: La resolución de acreditación para la prestación de servicios de certificación de Información contendrá al menos lo siguiente:*

a) Descripción de los servicios autorizados;

b) Características técnicas y legales relativas a la operación de los servicios de certificación de información y servicios relacionados autorizados;

c) Obligaciones y responsabilidades de las Entidades de Certificación de Información y Servicios Relacionados de acuerdo a lo establecido en la Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos;

d) Procedimientos para garantizar la protección de los usuarios aún en caso de extinción de la acreditación; y,

e) Causales de extinción de la acreditación."

*"**Art.** ...- Operación: Una vez otorgada y registrada la acreditación, la Entidad de Certificación de Información y Servicios relacionados dispondrá del plazo de seis (6) meses para iniciar la operación. Vencido dicho plazo la Superintendencia de Telecomunicaciones informará a la Secretaría Nacional de Telecomunicaciones si el titular de la acreditación ha incumplido con esta disposición, en cuyo caso se extinguirá la resolución de acreditación. La Entidad de Certificación de Información y Servicios Relacionados podrá pedir, por una sola vez, la ampliación del plazo para iniciar operaciones mediante solicitud motivada. Dicha ampliación, de concederse, no podrá exceder de 90 días calendario."*

*"**Art.** ...- Extinción de la acreditación: La acreditación se extinguirá por las siguientes causas:*

a) Terminación del plazo para la cual fue emitida;

b) Incumplimiento de las obligaciones por parte de la Entidad de Certificación de Información y Servicios Relacionados Acreditada;

c) Por resolución motivada del CONATEL, por causas técnicas o legales debidamente comprobadas, incluyendo la presentación de información falsa o alteraciones para aparentar cumplir los requisitos exigidos, así como la prestación de servicios o realizar actividades distintas a las señaladas en la acreditación;

d) Cese temporal o definitivo de operaciones de la Entidad Acreditada por cualquier causa; y,

e) Por las causas previstas en el Estatuto del Régimen Jurídico Administrativo de la Función Ejecutiva.

Una vez extinguida la acreditación el CONATEL podrá adoptar las medidas administrativas, judiciales y extrajudiciales que considere necesarias para garantizar la protección de la información de los usuarios y el ejercicio de los derechos adquiridos por estos."

*"**Art. ...-** Acreditación para Entidades del Estado.- Las instituciones y entidades del Estado, así como las empresas públicas, señaladas en la Constitución de la República, de acuerdo con la Disposición General Octava de la Ley, podrán prestar servicios como Entidades de Certificación de Información y Servicios Relacionados, previa resolución emitida por el CONATEL.*

Las instituciones públicas obtendrán certificados de firma electrónica de las entidades de Certificación de Información y Servicios Relacionados Acreditadas, de derecho público o de derecho privado."

*"**Art. ...-** Garantía de Responsabilidad: De conformidad con lo dispuesto en el apartado h) del artículo 30 de la Ley No. 67, las Entidades de Certificación de información y, Servicios Relacionados Acreditadas deberán contar con una garantía de responsabilidad para asegurar a los usuarios el pago de los daños y perjuicios ocasionados por el incumplimiento de las obligaciones. Esta garantía será incondicional, irrevocable y de cobro inmediato y podrá consistir en pólizas de seguro de responsabilidad previstas en el artículo 43 de la Codificación de la Ley General de Seguros u otro tipo de garantías que están autorizadas conforme lo dispuesto en el artículo 51, letra c) de la Ley General de Instituciones del Sistema Financiero.*

Como parámetros iniciales se establecen:

a) Para el primer año de operaciones, la Entidad de Certificación de Información y Servicios Relacionados Acreditada, deberá contratar y mantener, a favor de la Secretaría Nacional de Telecomunicaciones, una garantía de responsabilidad para asegurar a los usuarios el pago de los daños y perjuicios ocasionados por el posible incumplimiento de las obligaciones, cuyo monto será igual o mayor a cuatrocientos mil dólares de los Estados Unidos de América (USD $ 400.000,00). En el contrato de prestación de servicios que suscriba la Entidad de Certificación de información con los usuarios, se deberá incluir una cláusula relacionada con los aspectos de esta garantía, tales como: monto asignado a cada usuario, mecanismos de reclamación y restitución de valores.

b) Para el segundo año de operaciones y hasta la finalización del plazo de la acreditación, la Entidad de Certificación de Información y Servicios Relacionados Acreditada deberá contratar a favor de la Secretaría Nacional de Telecomunicaciones, una garantía, cuyo monto estará en función de un valor base de garantía por certificado y que será determinado por el CONATEL.

En la regulación que emita el CONATEL para establecer el valor base de garantía de responsabilidad por certificado, se considerará la evolución del mercado y la protección de los derechos de los usuarios, observando lo dispuesto en el artículo 31 de la Ley. No. 67.

La Entidad de Certificación de Información y Servicios Relacionados Acreditada quedará exenta de responsabilidad por daños y perjuicios cuando el usuario exceda los límites de uso indicados en el certificado.

La Entidad de Certificación de Información y Servicios Relacionados Acreditada, previo al inicio de las operaciones, remitirán a la Secretaría Nacional de Telecomunicaciones, a satisfacción de ésta, el original de la garantía. Asimismo, durante el plazo de vigencia de la acreditación dichas Entidades remitirán a la Secretaría Nacional de Telecomunicaciones,

hasta el 31 de enero de cada año, el original de la garantía mencionada en el apartado b) del presente artículo."

*"**Art. ...-** Control: La Superintendencia de Telecomunicaciones realizará los controles necesarios a las Entidades de Certificación de Información y Servicios Relacionados así como a los Terceros Vinculados, con el objeto de garantizar el cumplimiento de la normativa vigente y de los términos y condiciones de autorización y registro.*

Supervisará e inspeccionará en cualquier momento las instalaciones de los prestadores de dichos servicios, para lo cual deberán brindar todas las facilidades y proporcionar la información necesaria para cumplir con tal fin; de no hacerlo estarán sujetos a las sanciones de ley."

*"**Art. 18.-** Responsabilidades de las entidades de certificación de información.- Es responsabilidad de la entidad certificadora de información o del tercero vinculado que actúe en su nombre, verificar la autenticidad y exactitud de todos los datos que consten en el certificado de firma electrónica.*

El CONATEL podrá requerir en cualquier momento de la entidad de certificación de información, del tercero vinculado 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.

La Entidad de Certificación de Información y Servicios Relacionados Acreditada no podrá ceder o transferir total ni parcialmente los derechos o deberes derivados de la acreditación.

Es responsabilidad de las Entidades de Certificación de Información y Servicios Relacionados Acreditadas emitir certificados únicos. Cada certificado deberá contener un identificador exclusivo que lo distinga de forma unívoca ante el resto y solo podrán emitir certificados vinculados a personas naturales mayores de edad, con plena capacidad de obrar. Está prohibida la emisión de certificados de prueba o demostración.

El formato de los contratos que las Entidades de Certificación de Información y Servicios Relacionados suscriban con los usuarios, deberán ser remitidos a la Secretaría Nacional de Telecomunicaciones, previo al inicio de operaciones o cuando dicho formato sea modificado."

Resolución 479-20-CONATEL-2008, de 08 de octubre de 2008, expide el Reglamento para la Organización y Funcionamiento del Registro Público Nacional de Entidades de Certificación de Información y Servicios Relacionados Acreditadas y Terceros Vinculados, señala:

*"**Art. 11.-** El plazo para iniciar la operación se contará a partir del día siguiente al de la fecha de notificación por parte de la Dirección General de Gestión de los Servicios de Telecomunicaciones de la Secretaría Nacional de Telecomunicaciones, de la inscripción del acto administrativo de acreditación de la entidad de certificación de información y servicios relacionados."*

*"**Art. 18.-** La inscripción de entidades de certificación de información y servicios relacionados acreditadas contendrá por lo menos la siguiente información:*

a. Nombre, razón social o denominación de la entidad de certificación de información y servicios relacionados acreditada;

b. Dirección legal de la entidad de certificación de información y servicios relacionados acreditada, incluyendo número telefónico, así como también una dirección de correo electrónico;

c. Nombres y apellidos completos del representante legal de la entidad de certificación de información y servicios relacionados acreditada;

d. Número y fecha de la resolución de acreditación;

e. Servicios que va a prestar y plazo de duración de la acreditación;

f. Número de tomo, página, acta; y fecha de inscripción;

g. Número de registro único de contribuyentes; y,

h. Características técnicas de operación o prestación de servicios, así como el ámbito de aplicación y modalidad de los servicios."

2. ANÁLISIS:

De la revisión a la petición ingresada en este Organismo Técnico de Regulación y Control de las Telecomunicaciones suscrita por la señora Economista Verónica Artola Jarrín Gerente General del Banco Central del Ecuador por medio del cual solicitó la renovación de la Acreditación del Banco Central del Ecuador como Entidad de Certificación de Información y Servicios Relacionados, se puede determinar que ha cumplido con los requisitos establecidos en el tercer, articulo innumerado posterior al artículo 17 del Reglamento General a la Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos, reformado con Decreto Ejecutivo No. 1356 de 29 de septiembre de 2008, publicado en el Registro Oficial 440 de 06 de octubre de 2008, los cuales se detallan a continuación:

- Solicitud dirigida a la Agencia de Regulación y Control de las Telecomunicaciones, ingresada con trámite No. ARCOTEL-CTDS-2018-0009-E de 06 de julio de 2018, suscrita por la señora Economista Verónica Artola Jarrín Gerente General del Banco Central del Ecuador, por medio del cual solicitó la Acreditación del Banco Central del Ecuador como Entidad de Certificación de Información y Servicios Relacionados.

- Copia de la Cédula de Ciudadanía No. 171299969-5 de la señora Economista Verónica Artola Jarrín Gerente General del Banco Central del Ecuador.

- Copia del certificado de votación No. 001-249 de la señora Economista Verónica Artola Jarrín Gerente General del Banco Central del Ecuador.

INFORMACIÓN GENERAL	
Entidad de Certificación de Información y Servicios Relacionados:	**Banco Central del Ecuador**
Nombres y apellidos del Representante Legal:	**Econ. Verónica Elizabeth Artola Jarrín**
Dirección:	**Ecuador. Quito. Av. 10 de Agosto N11-409 y Briceño. Edificio del Banco Central del Ecuador.**

- **RUC del Banco Central:** 1760002600001

- **El Informe Técnico concluye que:** *"La Entidad de Certificación de Información y Servicios Relacionados del Banco Central del Ecuador, ha cumplido con las obligaciones contractuales y normativas establecidas en la Acreditación otorgada conforme lo establece la Ley de Comercio Electrónico, por lo que técnicamente sería factible renovar la Acreditación de Entidad de Certificación de Información y Servicios Relacionados a favor del Banco Central del Ecuador."*

- **El Informe Económico – Financiero concluye que:** *"El Banco Central del Ecuador ha cumplido hasta la fecha con sus obligaciones económicas con la ARCOTEL y demuestra que tiene la capacidad económica y financiera para*

continuar con la prestación de servicios de certificación de información y servicios relacionados."

- **Obligaciones económicas**: Mediante memorando Nro. ARCOTEL-CTDG-2018-0530-M de 02 de octubre de 2018, la Dirección Técnica de Gestión Económica de Títulos Habilitantes, respecto a las Obligaciones Económicas del BANCO CENTRAL DEL ECUADOR señala: *"Una vez analizada la información proporcionada por la Coordinación Administrativa Financiera, mediante memorando Nro. ARCOTEL-CAFI-2018-0683-M de 25 de septiembre de 2018, así como el registro histórico de pagos obtenido del SIFAF (impresión de pantalla), adjunto al memorando indicado; se concluye que el BANCO CENTRAL DEL ECUADOR, no mantiene obligaciones pendientes de pago con ARCOTEL.*

  Cabe señalar, que con oficio Nro. BCE-DNSF-2018-0702-OF de 27 de septiembre de 2018, el Director Nacional de Servicios Financieros del Banco Central del Ecuador, presenta una póliza de Responsabilidad Civil con vigencia hasta el 31 de diciembre de 2018."

Por lo que se concluye que el Banco Central del Ecuador cumple con los requisitos respectivos determinados en el artículo innumerado posterior al artículo 17 del Reglamento General a la Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos.

3. CONCLUSION:

El Banco Central del Ecuador es una Entidad de Certificación de Información y Servicios Relacionados (ECIBCE) acreditada por el ex Consejo Nacional de Telecomunicaciones, mediante Resolución 481-20-CONATEL-2008 de 08 de octubre de 2008 y acto administrativo suscrito el 06 de noviembre de 2008, cuyo título habilitante fenece el 06 de noviembre de 2018.

Habiéndose cumplido con los requisitos que establece la Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos, así como su Reglamento General de aplicación, esta Dirección con sustento en los informes Técnico, Económico-Financiero y Jurídico recomienda a la Dirección Ejecutiva, la renovación de Acreditación como Entidad de Certificación y Servicios Relacionados, a favor del Banco Central del Ecuador, previo al pago establecido en la Ley ibídem se proceda con el registro y notificación correspondiente.

Para el efecto se adjunta el respectivo Proyecto de Resolución.

Firmo por delegación de la Dirección Ejecutiva de la ARCOTEL, según consta en la Resolución No. ARCOTEL-2016-0655 de 10 de agosto de 2016.

Aprobado por:

Ing. Carlos Vinicio Altamirano Freire
DIRECTOR TÉCNICO DE TÍTULOS HABILITANTES DE SERVICIOS Y REDES DE TELECOMUNICACIONES

INFORME TECNICO	INFORME ECONÓMICO	INFORME JURÍDICO	REVISADO
Elaborado por:	Elaborado por:	Elaborado por:	
Ing. Xavier Páez	Ing. Jose Prieto	Mgs. Carmiña Valle	Ing. Xavier Páez