

REGISTRO OFICIAL

ÓRGANO DE LA REPÚBLICA DEL ECUADOR

SUMARIO:

Págs.

FUNCIÓN EJECUTIVA

RESOLUCIONES:

BANCO CENTRAL DEL ECUADOR:

BCE-GG-002-2021 Apruébese el “IG-051 Declaración de Prácticas de Certificación - DPC” y otro 2

FUNCIÓN DE TRANSPARENCIA Y CONTROL SOCIAL

SUPERINTENDENCIA DE BANCOS:

SB-DTL-2021-0474 Califíquese como auditor externo al ingeniero en finanzas, Diego Ramiro Vallejo Arteaga..... 97

RESOLUCIÓN ADMINISTRATIVA No. BCE-GG- 002 -2021**GERENTE GENERAL
BANCO CENTRAL DEL ECUADOR****CONSIDERANDO:**

- Que, la Constitución de la República del Ecuador, en el artículo 226, dispone: *"(...) 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 (...)"*;
- Que, el artículo 26 del Código Orgánico Monetario y Financiero determina que: *"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, cuya organización y funciones están determinadas en la Constitución de la República, el citado Código, su Estatuto, las regulaciones expedidas por la Junta de Política y Regulación Monetaria y Financiera y los reglamentos internos"*;
- Que, el Código Orgánico Monetario y Financiero, en su artículo 36 numeral 40 determina: *"Funciones. - El Banco Central del Ecuador. Tiene las siguientes funciones: 40. Las demás que le asigne la ley y la Junta de Política y Regulación Monetaria y Financiera"*;
- Que, los numerales 1, 2 y 5 del artículo 49 del Código Orgánico Monetario y Financiero establecen como funciones del Gerente General del Banco Central: *"1. Ejercer la representación legal, judicial y extrajudicial del Banco Central del Ecuador. 2. Dirigir, coordinar y supervisar la gestión técnica, operativa y administrativa del Banco Central del Ecuador, para lo cual expedirá los reglamentos internos correspondientes. 5. Vigilar el cumplimiento de las regulaciones que dicte la Junta de Política y Regulación Monetaria y Financiera, en el ámbito de su competencia"*;
- Que, la Disposición General Segunda del Capítulo XV: Del Servicio de Entidad de Certificación de Información y Emisión de Certificados digitales o electrónicos, del Libro I: Sistema Monetario y Financiero, de la Codificación de Resoluciones Monetarias, Financieras, de Valores y Seguros expedida por la Junta de Política y Regulación Monetaria y Financiera; establece: *"Facúltase al Gerente General del Banco Central del Ecuador para que establezca los servicios de firma electrónica y relacionados que desarrolle la Entidad de Certificación y expida los reglamentos, manuales y demás normativa necesaria para la cabal y efectiva aplicación de la presente Regulación, entre los cuales deberá constar una que contenga las Declaraciones de Prácticas de Certificación y Políticas de Certificados"*;
- Que, el Banco Central del Ecuador es la "Entidad de Certificación de Información y Servicios Relacionados", acreditada por el Consejo Nacional de Telecomunicaciones (CONATEL) con Resolución 481-20-CONATEL-2008 del 8 de octubre de 2008; cuya Acreditación se renovó con Resolución No. ARCOTEL-2018-0902 de 25 de octubre de 2018 emitida por la

Agencia de Regulación y Control de las Telecomunicaciones, ARCOTEL, para un nuevo período de 10 años;

Que, el Art. 33 de la Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos, determina que los servicios de certificación de la información pueden ser proporcionados por un tercero vinculado, que demuestre su relación contractual con una Entidad de Certificación de Información y Servicios debidamente acreditada ante el CONATEL, actualmente ARCOTEL;

Que, en el artículo 3 de la Resolución No. ARCOTEL-2018-0902, la Entidad Acreditada para prestar Servicios de Certificación de Información y Servicios Relacionados, tendrá la siguiente responsabilidad: *"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 (...)"*;

Que, en el artículo 4 de la Resolución citada anteriormente, la Entidad Acreditada para prestar Servicios de Certificación de Información y Servicios Relacionados, tiene como una de sus obligaciones: *"6. Mantener actualizada 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 los 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 los usuarios."*

Que, el artículo 3 de la Ley Orgánica para la Optimización y Eficiencia de Trámites Administrativos prevé como principios a observar en los trámites administrativos, los siguientes: *"1. Celeridad. - Los trámites administrativos se gestionarán de la forma más eficiente y en el menor tiempo posible, sin afectar la calidad de su gestión (...) 11. Simplicidad. - Los trámites serán claros, sencillos, ágiles, racionales, pertinentes, útiles y de fácil entendimiento para los ciudadanos. Debe eliminarse toda complejidad innecesaria (...) 13. No duplicidad. - La información o documentación presentada por la o el administrado en el marco de la gestión de un trámite administrativo, no le podrá ser requerida nuevamente por la misma entidad para efectos de atender su trámite o uno posterior. 14. Mejora continua. - Las entidades reguladas por esta Ley deberán implementar procesos de mejoramiento continuo de la gestión de trámites administrativos a su cargo, que impliquen, al menos, un análisis del desempeño real de la gestión del trámite y oportunidades de mejora continua"*;

Que, los artículos 9 y 10 de la Ley Orgánica para la Optimización y Eficiencia de Trámites Administrativos regulan la Presunción de veracidad y Responsabilidad de la información, proporcionada por el usuario, es de su exclusiva responsabilidad, sin perjuicio de las consecuencias administrativas, civiles y penales que se generen por faltar a la verdad en lo declarado o informado;

Que, el inciso primero del artículo 11 de la Ley Orgánica para la Optimización y Eficiencia de Trámites Administrativos, establece: *"Entrega de datos o documentos. - En la gestión de*

trámites administrativos, las entidades reguladas por esta Ley no podrán exigir la presentación de originales o copias de documentos que contengan información que repose en las bases de datos de las entidades que conforman el Sistema Nacional de Registro de Datos Públicos o en bases develadas por entidades públicas.";

Que, el Estatuto del Régimen Jurídico Administrativo de la Función Ejecutiva, en el artículo 99, dispone: *"Los actos normativos podrán ser derogados o reformados por el órgano competente para hacerlo cuando así se lo considere conveniente. Se entenderá reformado tácitamente un acto normativo en la medida en que uno expedido con posterioridad contenga disposiciones contradictorias o diferentes al anterior. La derogación o reforma de una ley deja sin efecto al acto normativo que la regulaba. Así mismo, cuando se promulga una ley que establece normas incompatibles con un acto normativo anterior éste pierde eficacia en todo cuanto resulte en contradicción con el nuevo texto legal.";*

Que, mediante Informe Técnico No. BCE-SGSERV-2021-004 / BCE-DNSF-201-2021 de 24 de febrero de 2021, la Dirección Nacional de Servicios Financieros, a través de la Subgerencia de Servicios, concluyó y recomendó: *"La Entidad de Certificación de Información del Banco Central del Ecuador (ECIBCE), a través de la Dirección Nacional de Servicios Financieros, requiere realizar inclusiones y/o modificaciones a la Declaración de Prácticas de Certificación y a la Política de Certificado de Firma Electrónica de Persona Natural (...) con la finalidad de aprobar la sexta versión del "IG-051 Declaración de Prácticas de Certificación - DPC" y del "IG-052 Políticas de Certificado - PC Certificado de Firma Electrónica de Persona Natural de la Entidad de Certificación de Información del Banco Central del Ecuador - ECIBCE", se recomienda a la Gerencia General aprobar el proyecto de Resolución Administrativa que acompaña a este informe";*

Que, a través de Informe Jurídico No. BCE-CGJ-013-2021 de 01 de marzo de 2021, la Coordinación General Jurídica concluyó que: *"la propuesta presentada por la Subgerencia de Servicios y la Dirección Nacional de Servicios Financieros a través del Informe Técnico BCE-SGSERV-2021-004 / BCE-DNSF-201-2021, se considera legalmente procedente conforme el ámbito de atribuciones y competencias del Banco Central del Ecuador";*

Que, mediante Resolución No. 386-2017-G de 1 de junio de 2017, la Junta de Política y Regulación Monetaria y Financiera designó a la economista Verónica Artola Jarrín como Gerente General del Banco Central del Ecuador;

En ejercicio de sus funciones y atribuciones:

RESUELVE:

ARTÍCULO 1: Aprobar el "IG-051 Declaración de Prácticas de Certificación - DPC" de la Entidad de Certificación de Información del Banco Central del Ecuador (ECIBCE) Versión 6.0, de acuerdo a lo descrito en el Anexo 1 de la presente resolución.

ARTÍCULO 2: Aprobar el “IG-052 Políticas de Certificado - PC Certificado de Firma Electrónica de Persona Natural de la Entidad de Certificación de Información del Banco Central del Ecuador - ECIBCE” Versión 6.0, de acuerdo a lo descrito en el Anexo 2 de la presente resolución.

DISPOSICIÓN GENERAL. - Encárguese de la ejecución y cumplimiento de la presente resolución a la Dirección Nacional de Servicios Financieros y la Subgerencia de Servicios del Banco Central del Ecuador; y, a la Dirección de Gestión Documental y Archivo su publicación en el Registro Oficial.

DISPOSICIÓN DEROGATORIA. - Deróguese el instructivo de gerencia “IG-051 Declaración de Prácticas de Certificación DPC”, OID: 1.3.6.1.4.1.37947.1.1, Versión 5.0; y, el instructivo de gerencia “IG-052 Políticas de Certificado - PC Certificado de Firma Electrónica de Persona Natural de la Entidad de Certificación de Información del Banco Central del Ecuador - ECIBCE”, OID: 1.3.6.1.4.1.37947.2.1.1, Versión 5.0, Anexo 1 del Artículo 1 de la Resolución Administrativa No. BCE-GG-104-2019 de 13 de septiembre de 2019.

DISPOSICIÓN FINAL. - La presente Resolución entrará en vigencia a partir de su publicación en Registro Oficial.

COMUNÍQUESE. - Dada en la ciudad de Quito, Distrito Metropolitano, a los 09 días del mes de marzo de 2021.



Firmado electrónicamente por:

VERONICA
ELIZABETH
ARTOLA JARRIN

Econ. Verónica Artola Jarrín
GERENTE GENERAL
BANCO CENTRAL DEL ECUADOR

ANEXO 1



BANCO CENTRAL DEL ECUADOR

**IG-051 DECLARACIÓN DE
PRÁCTICAS DE
CERTIFICACIÓN - DPC
OID: 1.3.6.1.4.1.37947.1.1**

Marzo

2021

Este documento contiene la sexta versión de la Declaración de Prácticas de Certificación mismas que establecen el procedimiento normativo aplicable a la prestación de servicios de certificación de la Entidad de Certificación de Información Financieras del Banco Central del Ecuador.

Versión 6.0

**SUBGERENCIA DE SERVICIOS
DIRECCIÓN NACIONAL DE SERVICIOS FINANCIEROS
GESTIÓN DE CERTIFICACIÓN ELECTRÓNICA**

© 2021. Dirección de Procesos, Calidad e Innovación- Coordinación General de Planificación y Gestión Estratégica - Banco Central del Ecuador.

Todos los derechos reservados.

El presente documento no puede ser reproducido, distribuido, comunicado públicamente, archivado o introducido en un sistema de recuperación de información, o transmitido, en cualquier forma y por cualquier medio (electrónico, mecánico, fotográfico, grabación o cualquier otro), total o parcialmente, sin el previo consentimiento por escrito del Banco Central del Ecuador.

REVISIÓN Y APROBACIÓN.....	
CONTROL DE HISTORIAL DE CAMBIOS	
INFORMACIÓN GENERAL	
1. OBJETIVO	
2. BASE NORMATIVA.....	
3. GLOSARIO DE TÉRMINOS Y/O DEFINICIONES.....	
3.1. DEFINICIONES	
3.2. ACRÓNIMOS	
4. ÁMBITO DE APLICACIÓN	
5. CONTENIDO TÉCNICO DEL DOCUMENTO	
5.1. INTRODUCCIÓN	
5.1.1. Presentación y Alcance	
5.1.2. Normas, Estándares y RFC referenciados para la elaboración de la DPC	
5.1.3. Comunidad de Usuarios y Aplicabilidad.....	
5.1.3.1. Autoridad de Certificación	
5.1.3.2. Autoridad de Certificación Subordinada	
5.1.3.3. Autoridad de Registro (AR)	
5.1.3.4. Autoridad de Sellado de Tiempo	
5.1.3.5. Solicitante	
5.1.3.6. Suscriptor.....	
5.1.3.7. Usuario	
5.1.4. Tipos de Certificados.....	
5.1.4.1. Certificado de Firma Electrónica de Persona Natural	
5.1.4.2. Certificado de Firma Electrónica de Persona Jurídica	
5.1.4.3. Certificado de Estampado de Tiempo	
5.1.4.4. Certificado de Servidor Seguro SSL.....	
5.1.5. Garantía	
5.1.6. Fiabilidad de la Firma Electrónica a lo Largo del Tiempo.....	
5.1.7. Detalles de Contacto	
5.2. ASPECTOS GENERALES	
5.2.1. Obligaciones.....	
5.2.1.1. Obligaciones de la ECIBCE	

5.2.1.2. Obligaciones de la Autoridad de Registro (AR)	
5.2.1.3. Obligaciones del Solicitante	
5.2.1.4. Obligaciones del Suscriptor del Certificado de Firma Electrónica	
5.2.1.5. Obligaciones y Responsabilidades de los Usuarios	
5.2.1.5.1. Confianza en los Certificados	
5.2.2. Responsabilidades	
5.2.2.1. Responsabilidades de la Autoridad de Certificación (AC)	
5.2.2.2. Responsabilidades de la AR	
5.2.2.3. Responsabilidades del Suscriptor	
5.2.2.4. Responsabilidades del Usuario	
5.2.3. Políticas de Manejo de los Certificados de Firma Electrónica de la ECIBCE ...	
5.2.4. Interpretación y Ejecución	
5.2.4.1. Ley Aplicable	
5.2.4.2. Transferencia de certificados y Notificaciones	
5.2.5. Procedimiento de Resolución de Conflictos	
5.2.6. Tarifas de Servicios de Certificación Electrónica	
5.2.7. Publicación y Custodia	
5.2.7.1. Publicación de Información de la AC	
5.2.8. Confidencialidad y Protección de Datos	
5.2.8.1. Confidencialidad de las Claves de Firma Electrónica	
5.2.8.2. Confidencialidad en la Prestación de Servicios de Certificación	
5.2.9. Protección de Datos	
5.2.10. Derechos de Propiedad Intelectual	
5.3. GESTIÓN DE CLAVES	
5.3.1. Del Certificado de la AC Raíz y AC Subordinada de la ECIBCE	
5.3.1.1. Generación del Par de Claves	
5.3.1.2. Protocolo de Generación del Par de Claves	
5.3.1.3. Entrega de Clave Pública de la AC Raíz y AC Subordinadas a los Usuarios Finales	
5.3.1.4. Tamaño de las Claves	
5.3.1.5. Protección de Clave Privada de la AC Raíz y AC Subordinada de la ECIBCE	
36	
5.3.1.5.1. Control Multipersona de la Clave Privada	
5.3.1.5.2. Copia de Seguridad de la Clave Privada	

5.3.2.	De Certificados de Usuario Final	
5.3.2.1.	Generación del Par de Claves.....	
5.4.	SOLICITUD DE SERVICIOS DE CERTIFICACIÓN.....	
5.4.1.	Emisión de Certificados de Firma Electrónica.....	
5.4.2.	Emisión de Certificados para Servidor Seguro SSL.....	
5.5.	REVOCACIÓN Y SUSPENSIÓN DE CERTIFICADOS.....	
5.5.1.	Supuestos de Revocación	
5.5.1.1.	Efectos de la Revocación	
5.5.2.	Supuestos de Suspensión	
5.5.3.	Efectos y Límites de la Suspensión	
5.5.4.	Procedimiento de Suspensión y Revocación	
5.5.4.1.	Recepción de Solicitudes de Suspensión/Revocación	
5.5.4.2.	Decisión de Suspende/Revocar	
5.5.4.3.	Comunicación y Publicación de la Suspensión/Revocación	
5.6.	RECUPERACIÓN DEL CERTIFICADO	
5.6.1.	Supuestos de Recuperación:.....	
5.6.2.	Procedimiento de Recuperación.....	
5.7.	CADUCIDAD DE CERTIFICADOS.....	
5.8.	RENOVACIÓN DE LOS SERVICIOS DE CERTIFICACIÓN.....	
5.8.1.	Renovación de Certificados	
5.9.	EXTINCIÓN DE LA AC.....	
5.10.	CARACTERÍSTICAS DE LOS CERTIFICADOS Y DE LA LISTA DE CERTIFICADOS.....	
5.10.1.	Características de los Certificados	
5.10.2.	Lista de Certificados	
5.10.3.	Lista de Autoridades de Certificación Revocadas (ARL).....	
5.10.4.	Lista de Certificados Revocados (CRL).....	
5.11.	CONTROLES DE SEGURIDAD FÍSICA, PROCEDIMENTAL Y DE PERSONAL 52	
5.12.	FORMATOS	
5.13.	ACTUALIZACIÓN, PUBLICACIÓN Y NOTIFICACIÓN	
5.13.1.	Actualización de la Declaración de Prácticas de Certificación y de las Políticas de Certificados	
5.13.2.	Publicación de las Actualizaciones	
5.13.3.	Notificación de las Publicaciones.....	

REVISIÓN Y APROBACIÓN

Elaborado por:	Firma
Especialista de Certificación Electrónica 1	 Firmado electrónicamente por: VICTOR MARCELO BALAREZO NOBOA
Especialista Administrativo 1	 Firmado electrónicamente por: DARWIN HUMBERTO PAZMINO LUCIO
Revisado y Validado por:	Firma
Subgerente de Servicios	 Firmado electrónicamente por: JOHN CARLOS ARROYO JACOME
Directora Nacional de Servicios Financieros	 Firmado electrónicamente por: MARITZA IVON VASCONEZ LOPEZ
Especialista de Medios de Pago 2	 Firmado electrónicamente por: NANCY ESTHELA CONDE CASTILLO
Aprobado por:	Firma
Gerente General	

CONTROL DE HISTORIAL DE CAMBIOS

Versión	Descripción del cambio	Fecha de actualización
1.0	Versión inicial de la Declaración de Prácticas de Certificación - DPC OID: 1.3.6.1.4.1.37947.1.1	Julio - 2010
2.0	Actualización por disposición legal de la Declaración de Prácticas de Certificación - DPC OID: 1.3.6.1.4.1.37947.1.1	Marzo - 2011
3.0	Actualización por disposición legal de la Declaración de Prácticas de Certificación - DPC OID: 1.3.6.1.4.1.37947.1.1	Agosto - 2011
4.0	Actualización por disposición legal de la Declaración de Prácticas de Certificación - DPC OID: 1.3.6.1.4.1.37947.1.1	Noviembre - 2013
5.0	Actualización por disposición legal de la Declaración de Prácticas de Certificación - DPC OID: 1.3.6.1.4.1.37947.1.1	Marzo - 2018
6.0	Actualización de la Declaración de Prácticas de Certificación - DPC OID: 1.3.6.1.4.1.37947.1.1, se agrega el nuevo servicio de emisión en línea, política de requisitos conforme simplificación de trámites administrativos y actualización de cómputo de términos y plazos según lo establecido por el Código Orgánico Administrativo y comunicado mediante Circular Nro. BCE-CGJ-2020-0001-C de 08 de julio de 2020 y Memorando No. BCE-CGPGE-2020-0413-M de 03 de agosto de 2020.	Marzo - 2021

INFORMACIÓN GENERAL

TÍTULO	Declaración de Prácticas de Certificación - DPC - de la Entidad de Certificación de Información del Banco Central del Ecuador - ECIBCE OID: 1.3.6.1.4.1.37947.1.1
Autores:	Marcelo Balarezo Lorena Altamirano Dirección Nacional de Servicios Financieros
Vigencia:	El presente documento tendrá vigencia a partir de la fecha de su aprobación.
Aprobación:	Gerente General
Responsabilidad de la implementación, ejecución, del control previo y concurrente:	Subgerencia de Servicios. Dirección Nacional de Servicios Financieros. Gestión de Certificación Electrónica. Dirección Nacional de Riesgos de Operaciones. Dirección de Aseguramiento de la Calidad y Seguridad Informática. Gestión de Operación de Clave Pública.
Responsabilidad de la revisión y actualización:	El presente documento normativo será revisado y actualizado por las áreas previstas en <i>responsabilidad de la implementación, ejecución, del control previo y concurrente</i> .
Responsabilidad de la evaluación de control interno:	Dirección Nacional de Auditoría Interna Bancaria y/o Gubernamental, en el ámbito de su competencia.
Distribución:	El presente documento normativo será distribuido por la Dirección de Gestión Documental y Archivo a los servidores previstos en <i>responsabilidad de la implementación, ejecución, del control previo y concurrente</i> , para Terceros Vinculados a la ECIBCE y usuarios de Certificados de Firma Electrónica

1. OBJETIVO

Establecer el procedimiento normativo, aplicable a la prestación de servicios de certificación de la Entidad de Certificación de Información del Banco Central del Ecuador.

2. BASE NORMATIVA

- Constitución de la República del Ecuador.
- Código Orgánico Monetario y Financiero.
- Código Orgánico Administrativo.
- Ley Orgánica de Defensa del Consumidor.
- Ley Orgánica de Transparencia y Acceso a la Información Pública.
- Ley Orgánica para la Optimización y Eficiencia de Trámites Administrativos y su Reglamento General.
- Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos y su Reglamento.
- Codificación de Resoluciones emitidas por la Junta de Política y Regulación Monetaria y Financiera, Libro I: Sistema Monetario y Financiero, Título I, Capítulo XV “Del Servicio de Entidad de Certificación de Información y Emisión de Certificados Digitales o Electrónicos”.
- Codificación de las Normas de la Superintendencia de Bancos, Libro I, Título XII, Capítulo II Norma de Control para la Conservación de los Archivos en Sistemas de Almacenamiento de las Entidades Controladas por la Superintendencia de Bancos, expedida con Resolución No. SB-2016-698 del 14 de julio de 2016.
- Normas de Control Interno de la Contraloría General del Estado para las Entidades, Organismos del Sector Público y de las Personas Jurídicas de Derecho Privado que dispongan de Recursos Públicos.
- Acuerdo Ministerial No. 181 del 15 de septiembre de 2011, Acuerdo No. 006-2015 del 27 de enero de 2015 y Acuerdo No. 012-2016 emitidos por el Ministerio de Telecomunicaciones y de la Sociedad de la Información.
- Acuerdos Ministeriales o Resoluciones que expida el Ministerio de Telecomunicaciones y Sociedad de la Información MINTEL, sobre la materia.
- Resolución No. ARCOTEL-2018-0902 del 25 de octubre de 2018, mediante la cual se renovó la acreditación del Banco Central del Ecuador como Entidad de Certificación de la Información y Servicios Relacionados.
- Resoluciones y demás normativa conexas, expedida por la ARCOTEL.

- Estatuto Orgánico de Gestión Organizacional por procesos del Banco Central del Ecuador vigente.
- Resoluciones Administrativas del Banco Central del Ecuador.
- Normas Técnicas Ecuatorianas NTE INEN-ISO/IEC 27000 para la Gestión de Seguridad de la Información, según actualice el Instituto Ecuatoriano de Normalización.
- Normas para Administración de Seguridad de Información del Banco Central del Ecuador (NT-001) de 27 de diciembre de 2017.

3. GLOSARIO DE TÉRMINOS Y/O DEFINICIONES

3.1. DEFINICIONES

Acuerdo de Autoridad de Registro: Contrato suscrito entre la ECIBCE y una entidad interna o externa al Banco Central, sea ésta pública o privada, que tiene como objeto regular la relación jurídica entre ambos para cumplir actividades de emisión, revocación y renovación de Certificados Digitales por delegación de la ECIBCE; así como brindar otros servicios relacionados.

AC Raíz BCE: Autoridad de Certificación Raíz Banco Central del Ecuador, emite certificados a Autoridades de Certificación Subordinadas y firma CRL's y ARL's.

AC Subordinada: AC Banco Central del Ecuador, Autoridad de Certificación Subordinada del Banco Central del Ecuador, cuyo objetivo es emitir certificados a usuarios finales y firmar CRL's; así como certificados para autoridades de estampado de tiempo y OCSP.

Autoridad de Certificación (AC – en inglés CA, Certification Authority-): Es la entidad de confianza, responsable de emitir y revocar certificados digitales de firma electrónica y que puede prestar otros servicios relacionados como la publicación de certificados, publicación de listas de certificados revocados (CRLs), comprobación de validez de certificados, custodia electrónica, entre otros.

La prestación de servicios de certificación por parte de terceros será únicamente a través de la vinculación con una Entidad de Certificación Acreditada.

Autoridad de Registro (AR): Dependencia/Área del Banco Central del Ecuador o entidad pública/privada externa al Banco Central que en calidad de Tercero Vinculado a la ECIBCE, se encargará de recibir, validar, verificar y gestionar las solicitudes de emisión, revocación y renovación de certificados digitales de firma electrónica y otros servicios relacionados, cumpliendo con lo establecido en las políticas y procedimientos definidos en este documento y demás documentos normativos relacionados.

Autoridad de Sellado de Tiempo: Dependencia del Banco Central o entidad pública/privada externa al Banco Central que en calidad de Tercero Vinculado, se encargará de emitir Sellos Digitales de Tiempo, cumpliendo con lo establecido en la Ley de Comercio Electrónico, Firmas

Electrónicas y Mensajes de Datos; y en concordancia con las políticas y procedimientos definidos en este documento y demás documentos normativos relacionados.

Certificado Digital: Es un documento digital mediante el cual la autoridad de certificación asegura la vinculación entre la identidad del usuario, su clave pública y privada.

Certificado de Firma Electrónica: El Certificado de firma Electrónica es un archivo, que certifica la vinculación de una firma electrónica con una persona determinada, a través de un proceso de comprobación que confirma su identidad.

Certificados de Firma Electrónica de todo Propósito: Son certificados de firma electrónica que servirán para firmar electrónicamente: correos electrónicos, facturas electrónicas, contratos electrónicos, ofertas del Sistema Nacional de Contratación Pública, transacciones electrónicas, trámites tributarios electrónicos, trámites de importaciones y exportaciones o cualquier otro tipo de aplicaciones donde se pueda reemplazar la firma manuscrita y se encuentre facultado para hacerlo dentro del ámbito de su actividad o límites de su uso. Se puede utilizar también para autenticación y cifrado de datos. Este certificado, puede ser utilizado por personas naturales o físicas, así como Personas Jurídicas, Representante Legal, Miembro de Empresa o Empleado con relación de dependencia.

Certificado de Persona Natural o Física: Son certificados que identifican al suscriptor como una persona natural o física y será responsable a título personal de todo lo que firme electrónicamente, dentro del ámbito de su actividad y límites de uso que correspondan.

Certificado de Persona Jurídica, Representante Legal, Miembro de Empresa o Empleado con relación de dependencia (literal b, numeral 1.2.1, artículo 1 del Acuerdo Ministerial 181 reformado el 25 de enero de 2015 con Acuerdo Ministerial 006-2015): Son certificados que identifican al suscriptor, como una persona jurídica de derecho público y privado a través de su representación legal o de las personas que actúen en su representación, quienes serán responsables en tal calidad de todo lo que firme dentro del ámbito de su competencia y límites de uso que correspondan.

Certificados de Estampado de Tiempo: Son certificados que sirven para firmar electrónicamente estampas o sellos de tiempo de acuerdo a sus límites de uso. Este certificado, puede ser utilizado por quien adquiera el servicio de estampado de tiempo.

El estampado de tiempo es un mecanismo que permite probar la integridad de una serie de datos electrónicos, es decir, permite demostrar fehacientemente que esos datos han existido en un momento determinado, y que no han sido alterados desde entonces.

El tiempo es tomado de una fuente segura e independiente, en el caso de la ECIBCE, el tiempo es tomado del Instituto Oceanográfico de la Armada del Ecuador - INOCAR.

Certificado de Servidor Web: Son certificados emitidos a empresas privadas o entidades públicas que establecen conexiones por internet o redes privadas con clientes y que aseguran el canal de comunicación mediante su uso.

Certificado Reconocido: Certificado expedido por una Entidad de Certificación Acreditada por la autoridad competente, actualmente la ARCOTEL, que cumple los requisitos establecidos en la Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos, en cuanto a la comprobación de la identidad y demás circunstancias de los solicitantes y a la fiabilidad y las garantías de los servicios de certificación que presten.

Clave Pública y Clave Privada: La infraestructura de clave pública se basa en la criptografía asimétrica, la que emplea un par de claves (lo que se cifra con una de ellas sólo se puede descifrar con la otra y viceversa). A una de esas claves se la denomina pública y se la incluye en el certificado electrónico, mientras que a la otra se la denomina privada y únicamente es conocida por el titular del certificado.

Contenedor de Certificado de Firma Electrónica: El certificado de firma electrónica puede estar contenido en archivo digital (p12), roaming, dispositivo TOKEN, dispositivo criptográfico de seguridad HSM o en dispositivo móvil tipo Smartphone; éste último puede estar contenido mediante una aplicación (APP) que cumple con niveles de seguridad FIPS 140-1.

Contrato de Prestación de Servicios de Certificación: Contrato que tiene por objeto regular los derechos y obligaciones derivados de la prestación de los servicios de Certificación por la ECIBCE, al suscriptor.

Datos de Creación de Firma: Son datos únicos, como códigos o claves criptográficas privadas, que el suscriptor utiliza para crear la firma electrónica.

Datos de Verificación de Firma: Son los datos, como códigos o claves criptográficas públicas, que se utilizan para verificar la firma electrónica, mediante el uso de herramientas o aplicaciones destinadas para esta finalidad.

Declaración de Prácticas de Certificación (DPC): Documento que reúne las reglas que la Entidad de Certificación de Información utiliza para la gestión, administración, homologación, generación, uso y conservación de cada uno de los certificados de firma electrónica así como de los servicios relacionados que ofrece. Establecen el alcance de los servicios ofrecidos y las responsabilidades asumidas por todas las partes, estos son: La ECI, su(s) tercero(s) vinculado(s) y usuarios.

Dispositivo Criptográfico Portable Seguro - TOKEN: Elemento físico donde se almacena en forma segura (chip criptográfico) el certificado de firma electrónica que será emitido por la ECIBCE. 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*).

Distinguished Name: Nombre Distintivo, son los campos que sirve para identificar a un certificado digital, que además es único.

Documento de identidad válido: Cédula de Ciudadanía, Cédula de Identidad, Pasaporte y demás documentos que la legislación ecuatoriana admita como válidos para acreditar la identidad de una persona.

En línea: El concepto se utiliza en el ámbito de la informática para referirse a algo o a alguien que está haciendo uso de la red Internet.

Entidad de Certificación de información y servicios relacionados del Banco Central del Ecuador (ECIBCE): Es el Banco Central del Ecuador que emite certificados de firma electrónica y que puede prestar otros servicios relacionados con la firma electrónica, autorizada por el Consejo Nacional de Telecomunicaciones, según lo dispuesto en Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos y su Reglamento General.

Las autoridades de registro de la ECIBCE, serán las encargadas de la verificación de documentos e identificación de los solicitantes y suscriptores del certificado de firma electrónica, mediante el procedimiento definido vigente; para luego completar el proceso de emisión de certificados.

Estampas o Sellos de tiempo: Son registros de tiempo que se colocan o se plasman en los mensajes de datos o documentos suscritos con una firma electrónica, que confirma y asegura la fecha y hora de la existencia de dicho mensaje de datos o documento; este servicio es proporcionado y administrado por la Entidad de Certificación de Información.

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, amparado por la Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos.

FIPS: Federal Information Processing Standard, por sus siglas en inglés y son estándares de seguridad del Gobierno Estadounidense para el procesamiento de la información”; para el caso de la ECIBCE y ésta DPC, son niveles de seguridad requeridos para el dispositivo TOKEN que puede comprender todo el dispositivo criptográfico; a nivel externo, de 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. Los FIPS son avalados por el NIST (*National Institute of Standards and Technology*).

Identificación: Reconocimiento fehaciente de la identidad del suscriptor del signatario de un certificado.

Lista de Certificados Revocados - CRL: Es una lista de certificados que han sido revocados, que no son válidos y en los que no debe confiar ningún usuario del sistema.

Módulo de seguridad criptográfico: (HSM- Hardware Security Module). Empleado para almacenar claves y realizar operaciones criptográficas de modo seguro, aporta aceleración de hardware para operaciones criptográficas.

NITS: *National Institute of Standards and Technology*, por sus siglas en inglés, Instituto Nacional de Normas y Tecnología - es una agencia de la Administración de Tecnología del Departamento de Comercio de los Estados Unidos (*cuya misión es promover la innovación y la competitividad industrial EE.UU. haciendo avanzar la ciencia de medición, normas, y la tecnología de forma que mejoren la seguridad económica y calidad de vida*).

OCSP: Online Certificate Status Protocol (OCSP) es un servicio para determinar el estado de vigencia de un certificado, mediante consulta en línea a los servidores de confianza de la ECIBCE.

Persona Natural o Física: Son personas todos los individuos de la especie humana, cualquiera que sea su edad, sexo o condición.

Persona Jurídica: Es una persona ficticia, capaz de ejercer derechos y contraer obligaciones y de ser representada judicial y extrajudicialmente.

PKI: En criptografía, una infraestructura de clave pública, acrónimo en inglés, PKI Public Key Infrastructure, es una combinación de un conjunto de elementos: hardware, software, personas, políticas y procedimientos de seguridad que permiten la ejecución, de operaciones criptográficas como el cifrado, como la firma digital o el no repudio de transacciones electrónicas.

Políticas de Certificados (PC): Contiene las reglas a las que se sujeta el uso de los certificados digitales definidos en la política. Se describen los papeles, responsabilidades y relaciones entre el usuario final y la Autoridad de Certificación y las reglas de solicitud, adquisición gestión y uso de los certificados. Este documento matiza y complementa a la Declaración de Prácticas de Certificación (DPC) de la Autoridad de Certificación.

Prestador de Servicios de Certificación: Empresa o Persona jurídica que expide certificados o presta otros servicios en relación con la firma electrónica.

Registro: Proceso directo por el cual el Solicitante o el Suscriptor consigna en una solicitud, toda la información relacionada con él.

Revocatoria: Dejar sin efecto o quitar la validez a un certificado digital de firma electrónica emitido por la ECIBCE, conforme señala la Ley de Comercio Electrónico, Firmas y Mensaje de Datos y su reglamento, esta DPC y Políticas de Certificados (PC).

Secure Sockets Layer - SSL: Es un protocolo criptográfico que proporciona comunicación segura por una red, comúnmente Internet.

Servidor: Es una computadora que, formando parte de una red, provee servicios a otras computadoras denominadas clientes.

Solicitante: La persona natural o jurídica que solicita la emisión de un Certificado por parte de la ECIBCE, sometiéndose al procedimiento de verificación de identidad y de creación del certificado de firma electrónica que la ECIBCE ha establecido para su emisión.

Suscriptor: El suscriptor será la persona natural o jurídica a favor de la cual se ha emitido un certificado. Los suscriptores deberán ajustarse a lo señalado en la DPC, en la PC del certificado que han obtenido y, en su caso, en el contrato de Prestación de Servicios suscrito con la ECIBCE los suscriptores deberán ajustarse a los procedimientos establecidos para la petición de cada tipo de certificado, y cumplir los requisitos que se establezcan en esta DPC.

Servicios Relacionados: Son servicios complementarios a la firma electrónica brindados por una entidad de certificación acreditada por el CONATEL. Para la ECIBCE son: Sellado de tiempo, aplicaciones y librerías para uso de firma electrónica y sellado de tiempo, certificados de servidor seguro entre otros.

Tercero Vinculado: Con sujeción al artículo 33 de la Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos, la Prestación de Servicios de Certificación de información podrá ser proporcionada por parte de terceros, para lo cual deberá demostrar su vinculación con la Entidad de Certificación de Información y Servicios Relacionados Acreditada ante el CONATEL.

Usuario: La persona natural o persona jurídica que voluntariamente confía o hace uso de un certificado de firma electrónica emitido por la ECIBCE, le será de aplicación el presente documento.

X.500: Es un conjunto de estándares de redes de ordenadores de la ITU-T sobre servicios de directorio

X.509: Especifica formatos estándar para certificados de claves públicas y un algoritmo de validación de la ruta de certificación.

3.2. ACRÓNIMOS

AC: Autoridad de Certificación.

AR: Autoridad de Registro (BCE o Tercero Vinculado)

ARL: Lista de autoridades de certificación revocadas.

BCE: Banco Central del Ecuador.

C: Country (País). Atributo del Nombre Distintivo (DN) de un objeto dentro de la estructura de directorio X.500.

CN: Common Name (Nombre Común). Atributo del Nombre Distintivo (DN) de un objeto dentro de la estructura de directorio X.500.

CRL: Certificate Revocation List. Lista de Certificados Revocados.

CSR: Certificate Signing Request. Petición del certificado.

DN: Distinguished Name (Nombre Distintivo). Identificación unívoca de una entrada dentro de la estructura de directorio X.500.

DPC: Declaración de Prácticas de Certificación.

DPC-ST: Declaraciones de Prácticas de Certificación - Sellado de Tiempo.

ECI: Entidad de Certificación de Información.

ECIBCE: Entidad de Certificación de Información del Banco Central del Ecuador.

ETSI: European Telecommunications Standard Institute.

FIPS: Federal Information Processing Standard. Estándares del Gobierno Norteamericano para el procesamiento de la información.

HSM: Hardware Security Module. Módulo de seguridad criptográfico empleado para almacenar claves y realizar operaciones criptográficas de modo seguro.

ISO: International Organization for Standardization.

ITU-T o UIT: Unión Internacional de Telecomunicaciones que es el organismo especializado en telecomunicaciones de la Organización de las Naciones Unidas, encargado de regular las telecomunicaciones a nivel internacional entre las distintas administraciones y empresas operadoras.

L: Localidad. Atributo del Nombre Distintivo (DN) de un objeto dentro de la estructura de directorio X.500.

LDAP: Lightweight Directory Access Protocol. Protocolo de acceso a servicios de directorio.

O: Organization. Atributo del Nombre Distintivo (DN) de un objeto dentro de la estructura de directorio X.500.

OCSP: Online Certificate Status Protocol. Este protocolo permite comprobar en línea la vigencia de un certificado electrónico.

OID: Object identifier. Identificador de objeto único.

ORGANISMO DE CONTROL: Agencia de Regulación y Control de las Telecomunicaciones, actualmente ARCOTEL.

OU: Organizational Unit. Atributo del Nombre Distintivo (DN) de un objeto dentro de la estructura de directorio X.500.

PC: Políticas de Certificados.

PIN: Personal Identification Number. Número de Identificación Personal o contraseña.

PKCS: Public Key Cryptography Standards. Estándares de PKI desarrollados por RSA Laboratories y aceptados internacionalmente, que define los diferentes tipos de formatos de firma electrónica.

PKI: Public Key Infrastructure. Infraestructura de Clave Pública.

PKIX: Grupo de trabajo del IETF. Public Key Infrastructure X509 IETF Working Group. Constituido con el objeto de desarrollar las especificaciones relacionadas con las PKI e Internet.

RFC: Request For Comments. Estándar emitido por la IETF.

SN: SurName. Apellido. Atributo del Nombre Distintivo (DN) de un objeto dentro de la estructura de directorio X.500.

SSL: Secure Sockets Layer. Protocolo para comunicación segura.

TSA: Time Stamping Authority. Autoridad de Sellado de Tiempo.

TST: Time stamp TOKEN. Sello Digital de Tiempo.

UTF8: Unicode Transformation Format - 8 bits.

4. ÁMBITO DE APLICACIÓN

- Oficina Matriz Quito
- Direcciones Zonales del BCE de Guayaquil y Cuenca
- Terceros Vinculados
- Usuarios de certificados electrónicos

5. CONTENIDO TÉCNICO DEL DOCUMENTO

5.1. INTRODUCCIÓN

5.1.1. Presentación y Alcance

El presente documento, constituye la Declaración de Prácticas de Certificación (DPC) de la ECIBCE, donde se definen los mecanismos relacionados con la operación de certificación electrónica. Esta Declaración de Prácticas de Certificación (DPC) cumple con lo dispuesto en la Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos y su Reglamento.

Esta Declaración de Prácticas de Certificación (DPC) presenta las prácticas que la ECIBCE y sus Autoridades de Registro (AR) prestan en relación a los servicios de certificación electrónica, las Políticas de Certificados que se utilizan para la emisión y gestión de certificados y en el mantenimiento de una infraestructura de clave pública (PKI) basada en certificados digitales o electrónicos. La DPC detalla y controla el proceso de certificación.

Las Políticas de Certificados (PC) abarcan la emisión, la gestión, la utilización, la revocación y la renovación de certificados. La DPC describe los términos para el cumplimiento de la legislación aplicable, las obligaciones legales y, proporciona información a todas las partes que crean, utilizan y validan certificados en el contexto de las PCs. Las partes que actúan en las PCs de la ECIBCE están ligadas a sus obligaciones en virtud de sus contratos con la ECIBCE, las AR de la ECIBCE, Terceros Vinculados y las que emiten, gestionan, revocan y renuevan certificados conforme las DPC de la ECIBCE.

5.1.2. 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-21188:2018 “Infraestructura de llave pública para servicios financieros — Estructura de prácticas y políticas”.
- RFC 2560 “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)”.
- RFC - 6960 Internet X.509 Internet Public Key Infrastructure Online Certificate Status Protocol – OCSP
- RFC - 5280 Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile
- RFC - 7382. Template for a Certification Practice Statement (CPS) for the Resource PKI (RPKI)
- RFC - 3850 Secure/Multipurpose Internet Mail Extensions (S/MIME) Version 3.1 Certificate Handling
- RFC - 3628 Policy Requirements for Time-Stamping Authorities (TSAs)
- RFC 7822 – 5905 Network Time Protocol Version 4 (NTPv4) Extension Fields
- RFC - 5755 An Internet Attribute Certificate Profile for Authorization
- RFC - 4476 Attribute Certificate (AC) Policies Extension
- RFC - 5913 Clearance Attribute and Authority Clearance Constraints Certificate Extension

5.1.3. Comunidad de Usuarios y Aplicabilidad

5.1.3.1. Autoridad de Certificación

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 esta DPC.

El Banco Central del Ecuador es la Entidad de Certificación de Identidad o Autoridad de Certificación (CA) acreditada por la ARCOTEL, y para sus operaciones mantiene bajo su custodia un certificado raíz, que es un certificado autofirmado y a partir de este construye la Ruta de Certificación, es decir, la CA Raíz y sus subordinadas. Cada Ruta de Certificación es una rama de múltiples CA intermedias o subordinadas que puede administrar una PKI.

5.1.3.2. Autoridad de Certificación Subordinada

La ECIBCE establece Autoridades de Certificación Subordinadas para relacionar una determinada clave pública con un sujeto o entidad concretos a través de la emisión de un Certificado de

conformidad con los términos de esta DPC y de la Política de Certificación (PC) de cada tipo de Certificado.

5.1.3.3. Autoridad de Registro (AR)

La ECIBCE actúa como Autoridad de Registro (AR) y, comprobará las identidades de los solicitantes de acuerdo a lo descrito en esta DPC y al proceso definido, sea en sus áreas de atención al cliente o a través de Terceros Vinculados a la ECIBCE.

La ECIBCE podrá asignar la comprobación de identidades a las oficinas del BCE y/o de ser el caso a Terceros que se encuentren vinculados con la ECIBCE; que actúen como Autoridades de Registro. Las autoridades de registro comprobarán la identidad de los solicitantes de acuerdo con las normas de esta DPC, la PC, el acuerdo de AR y las responsabilidades y obligaciones establecidas en la Acreditación como Entidad de Certificación.

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.

Los servicios a proporcionar a través de terceros tendrán la finalidad de implementar mejoras; en especial en función de la evolución de estándares tecnológicos reconocidos internacionalmente, fiables y seguros, que cumplan con exigencias de seguridad, acorde a las mejores prácticas internacionales y que garantice la prestación de los servicios a los usuarios.

5.1.3.4. 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 DPC-ST.

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.

5.1.3.5. Solicitante

A los efectos de esta DPC, se entenderá por Solicitante a la persona natural o jurídica que solicita la emisión de un Certificado a la ECIBCE o un servicio relacionado, sometiéndose al procedimiento de verificación de identidad y de creación del certificado de firma electrónica que la ECIBCE ha establecido para su emisión, de forma directa y/o a través de un tercero vinculado contractualmente.

5.1.3.6. Suscriptor

El suscriptor será la persona natural o persona jurídica a favor de quien se ha emitido un certificado u otorgado un servicio relacionado por parte de la ECIBCE. Los suscriptores deberán ajustarse a lo señalado en esta DPC, la PC del Certificado que han obtenido y, en su caso, al contrato de Prestación de Servicios suscrito con la ECIBCE. Los suscriptores deberán ajustarse a

los procedimientos establecidos para la petición de cada tipo de certificado, y cumplir los requisitos que se establezcan en esta DPC.

5.1.3.7. Usuario

Se entiende por Usuario del Certificado a la persona natural o jurídica que voluntariamente confía o hace uso de los Certificados de la ECIBCE emitido en diferentes contenedores de certificados de firma electrónica (token, archivo, roaming, hsm y dispositivo móvil tipo smartphone). Cuando el Usuario decida voluntariamente confiar y hacer uso del certificado, le será de aplicación la presente DPC.

5.1.4. Tipos de Certificados

5.1.4.1. Certificado de Firma Electrónica de Persona Natural

Permite identificar a una persona natural, quien será responsable a título personal de todo lo que firme en forma electrónica, dentro del ámbito de su actividad y límites de su uso que correspondan; por lo tanto, sirve para todo propósito dentro de las limitaciones legales y técnicas. Las políticas referentes a este tipo de certificado se encuentran en la correspondiente PC.

Este certificado se emite en las siguientes modalidades: Dispositivos criptográficos seguros - TOKEN en estándar PKCS#11, HSM en estándar PKCS#10, Dispositivos Móviles (IOS y Android) en estándar PKCS#11, en Archivo en estándar PKCS#12 (P12 o PFX), en repositorio centralizado Roaming y otros dispositivos.

5.1.4.2. Certificado de Firma Electrónica de Persona Jurídica

Permite identificar a una persona jurídica de derecho privado o público, a través de su representante legal o de las personas que pertenecen a la empresa, con determinado cargo, quienes serán responsables en tal calidad de todo lo que firmen dentro del ámbito de su actividad y límites de uso que correspondan o asigne la empresa; por lo tanto, sirve para todo propósito dentro de las limitaciones legales y técnicas. Las políticas referentes a este tipo de certificado se encuentran en la correspondiente PC.

Este certificado se emite en las siguientes modalidades: Dispositivos criptográficos seguros - TOKEN en estándar PKCS#11, HSM en estándar PKCS#10, Dispositivos Móviles (IOS y Android) en estándar PKCS#11, en Archivo en formato PKCS#12 (P12 o PFX), repositorio centralizado Roaming y otros dispositivos.

5.1.4.3. Certificado de Estampado de Tiempo

Sirve para firmar electrónicamente estampas o sellos de tiempo únicamente. Permite identificar a una autoridad de estampado de tiempo, quien será responsable a título de la institución pública o privada que representa de todo lo que firme dentro del ámbito de su actividad y límites uso que correspondan. Las políticas referentes a este tipo de certificado se encuentran en la correspondiente DPC de estampado de tiempo.

Este certificado se emite en las siguientes modalidades: Dispositivos criptográficos seguros en estándar PKCS#10 (HSM).

5.1.4.4. Certificado 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.

SSL proporciona autenticación y privacidad de la información entre extremos sobre Internet mediante el uso de criptografía. Habitualmente, sólo el servidor es autenticado (es decir, se garantiza su identidad) mientras que el cliente se mantiene sin autenticar.

Este certificado se emite en la siguiente modalidad: Generación de un Request CSR en estándar PKCS#10 Offline.

5.1.5. Garantía

La Entidad de Certificación de Información y Servicios Relacionados (ECIBCE), sin perjuicio de la responsabilidad y garantía establecida en el artículo 31 de la Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos, garantiza que ha realizado todos los trámites necesarios para verificar que la información contenida en cualquier certificado emitido por la ECIBCE es correcta al tiempo de su emisión. La ECIBCE también garantiza que cualquier certificado será revocado si en cualquier momento la ECIBCE considera que los contenidos del mismo no son correctos o que el certificado y la clave asociada han sido comprometidos, manipulados o sean objeto de mal uso.

La naturaleza de los trámites que la ECIBCE realiza para verificar la información contenida en un certificado varía según los tipos de certificación emitidos. En todo caso los trámites efectuados por la ECIBCE serán suficientes a los efectos de esta garantía. La ECIBCE no da otras garantías.

5.1.6. Fiabilidad de la Firma Electrónica a lo Largo del Tiempo

Para garantizar la fiabilidad de una firma electrónica a lo largo del tiempo, ésta deberá ser complementada con la información del estado del certificado asociado en el momento en que la misma se produjo y/o información no repudiable incorporando un sello de tiempo, así como los certificados que conforman la cadena de confianza.

Esto implica que, si se requiere que una firma pueda ser validada a lo largo del tiempo, la firma electrónica que se genera ha de incluir evidencias de su validez para que no pueda ser repudiada. Para este tipo de firmas deberá existir un servicio que mantenga dichas evidencias, y será necesario solicitar la actualización de las firmas antes de que las claves y el material criptográfico asociado sean vulnerables.

La generación de una firma electrónica podrá incluir los siguientes elementos:

- **Sello de Tiempo:** Se ha de incluir en la firma un sello de tiempo emitido por una Tercera Parte de Confianza, TSA de la ECIBCE (Autoridad de Sellado de Tiempo). El sello de tiempo asegura que tanto los datos originales del documento como la información del estado de los certificados, se generaron antes de una determinada fecha. El formato del sello de tiempo debe seguir el estándar definido en la RFC 3161.
- **Información de Revocación:** La firma ha de incluir un elemento que asegura que el certificado de firma es válido. Este elemento será generado por una Tercera Parte de Confianza, en este caso por la ECIBCE. Y se lo podrá realizar a través del servicio de consulta en línea de estado de certificados OCSP y lista de certificados revocados CRL, servicios disponibles en la página web de la ECIBCE.

Es necesario que con posterioridad las firmas puedan renovarse y actualizar los elementos de confianza (sellos de tiempo) para dotar a las firmas electrónicas de validez a lo largo del tiempo, logrando de esta manera garantizar su fiabilidad.

5.1.7. Detalles de Contacto

Nombre	Entidad de Certificación de Información del Banco Central del Ecuador
Correo electrónico	eci@bce.ec
Dirección	Av.10 de Agosto N11-409 y Briceño
Número de teléfono	(593-2) 3938600 Ext. 2863, 2857, 2833, 2839
Casillero Postal	339
Sitio Web	www.eci.bce.ec

5.2. ASPECTOS GENERALES

5.2.1. Obligaciones

5.2.1.1. Obligaciones de la ECIBCE

- Emitir certificados electrónicos conforme a la Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos, y su Reglamento General, esta DPC y a las PCs correspondientes y a los estándares de aplicación vigentes.
- Emitir certificados cuyo contenido mínimo sea el definido en las Políticas de Certificados vigentes.
- Emitir certificados según la información que obra en su poder y libres de errores de entrada de datos.
- Mantener sus propias claves privadas bajo su exclusivo control empleando módulos de seguridad en hardware HSM, sistemas y productos fiables para almacenarlas de forma que garanticen su confidencialidad y los hagan inaccesibles a personas no autorizadas, evitando su pérdida o divulgación.

- Emitir los certificados solicitados de acuerdo con lo dispuesto en esta DPC, en las PCs de cada tipo de Certificado y, en su caso, en los contratos de prestación de servicios de certificación correspondientes y en el acuerdo y/o contrato para Autoridad de Registro.
- Utilizar sistemas y productos fiables que estén protegidos contra toda alteración y que garanticen la seguridad técnica, y en su caso, criptográfica de los procesos de certificación a los que sirven de soporte.
- Facilitar el acceso a las versiones vigentes de la DPC y de las PCs de cada tipo de certificados, publicadas en el Portal Web de la ECIBCE www.eci.bce.ec
- Ofrecer y mantener la infraestructura necesaria para los servicios de certificación, así como los controles de seguridad física, de procedimiento y personales necesarios para la práctica de la actividad de certificación.
- Publicar los certificados emitidos y/ o revocados según lo establecido en la Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos.
- Proteger los datos personales según lo establecido en la Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos.
- Proporcionar al solicitante de la emisión del certificado la información mínima necesaria para el uso de los certificados. Dicha información deberá transmitirse de forma gratuita, por escrito o por vía electrónica.
- Tomar medidas contra la falsificación de certificados y garantizar la confidencialidad de los datos de creación de firma durante el proceso de generación, así como su entrega por un procedimiento seguro al suscriptor.
- Utilizar sistemas fiables para almacenar certificados reconocidos que permitan comprobar su autenticidad e impedir que personas no autorizadas alteren los datos.
- No almacenar ni copiar los datos de creación de firma del suscriptor.
- Custodiar por cualquier medio seguro toda la información y documentación relativa a un certificado reconocido y las declaraciones de prácticas de certificación vigentes en cada momento, al menos durante 15 años contados desde el momento de su expedición, de manera que puedan verificarse las firmas efectuadas con el mismo. A estos efectos, la ECIBCE almacena en formato digital o en papel todas las versiones de la DPC publicada y copia del contrato de prestación de servicios entre la entidad de certificación de información y el suscriptor.
- Informar sobre las modificaciones de las Políticas de Certificados y de la Declaración Prácticas de Certificación a los usuarios, suscriptores y AR's que estén vinculadas a ella.
- Ofrecer y mantener la infraestructura tecnológica, tanto hardware como software, para garantizar la operación de la Entidad de Certificación, de acuerdo a los estándares internacionales.

- Implementar y mantener los requerimientos de seguridad impuestos a la clave privada de la ECIBCE, de acuerdo a estas Declaraciones de Prácticas de Certificación (DPC) y Políticas de Certificados.
- Aprobar o negar las solicitudes de emisión de certificados digitales de firma electrónica, de acuerdo con lo establecido en esta Declaración de Práctica de Certificación (DPC), en las Políticas de Certificados, normas y procedimientos de la ECIBCE.
- Poner a disposición de los usuarios la lista de certificados revocados (CRL), a través de la página Web <https://www.eci.bce.ec/CRL>.
- Llevar a cabo cada uno de los pasos que se describan en el procedimiento de emisión de certificados de firma electrónica.
- Efectuar la identificación y autenticación de los usuarios como pasos previos a la revocatoria de los certificados de firma electrónica o proporcionar en su lugar mecanismos de autogestión de revocatorias; y,
- Proteger los datos personales de los solicitantes y usuarios de certificados digitales o electrónicos.
- Todas aquellas obligaciones impuestas en la presente DPC y, en su caso, la Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos, su Reglamento y en la Acreditación recibida por el Organismo de Control.

5.2.1.2. Obligaciones de la Autoridad de Registro (AR)

La Autoridad de Registro (AR) o Tercero Vinculado asumirá las siguientes obligaciones de las cuales será responsable:

- Identificar y autenticar correctamente al solicitante, suscriptor o a la organización que represente, conforme a los procedimientos que se establecen en esta DPC y en las Políticas de cada tipo de Certificado, normas y procedimientos de la ECIBCE.
- Formalizar los contratos de prestación de servicios de certificación con el Suscriptor en los términos y condiciones que establezca la ECIBCE.
- Almacenar de forma segura y por un periodo de 15 años la documentación aportada en el proceso de emisión del Certificado y en el proceso de suspensión/revocación del mismo, en los términos y condiciones que se establezcan en esta DPC, en la PC de cada tipo de certificado y, en su caso, en el acuerdo o contrato para la Autoridad de Registro y procedimientos establecidos por la ECIBCE.
- Llevar a cabo cualquier otra función que le correspondan, a través del personal que sea necesario en cada caso, conforme se establece en esta DPC y en la PC cada tipo de Certificado y, en su caso, el acuerdo o contrato para Autoridad de Registro.

- En todo caso, la AR permitirá a ECIBCE el acceso a los archivos y/o realizará la entrega de los mismos de acuerdo a los procedimientos de conservación de los archivos asumidos por la AR y le dará el derecho a investigar cualquier sospecha de infracción de la DPC y/o de las PC por parte de la AR o cualquier poseedor de un Certificado.
- La AR y los poseedores de cualquier Certificado deberán informar a la ECIBCE inmediatamente de cualquier sospecha de infracción.
- Dar y/o permitir a la ECIBCE todos los accesos necesarios para validar, monitorear, observar y/o asegurar que aplicativos, sistemas o desarrollos implementados proporcionen entornos seguros ofrecidos y/o cumplan con estándares internacionales, en los procesos presenciales o en línea, a través de sistemas de validación biométrica, para los procesos de emisión, renovación o revocación de certificados digitales de firma electrónica que requieran los usuarios.

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

5.2.1.3. Obligaciones del Solicitante

- Abonar las tarifas de registro que correspondan en virtud de los servicios que se soliciten.
- Suministrar a la AR la información necesaria para realizar una correcta identificación, de acuerdo a lo establecido en la respectiva política de certificado.
- Confirmar la exactitud y veracidad de la información suministrada, autorizar expresamente a la ECIBCE y/o su Tercero Vinculado a verificar de ser necesario la autenticidad de la misma; y, en caso de falsedad autoriza se informe a las autoridades competentes.
- Notificar cualquier cambio en los datos aportados para la creación del certificado durante su periodo de validez. En especial, solicitar la revocatoria y obtener un nuevo certificado de firma electrónica en casos excepcionales como es el cambio de número de identificación o nombres que puedan dar lugar a su identificación inexacta.
- Solicitar el Certificado según se estipula en los términos y condiciones que se establezcan en la PC de cada tipo de Certificado y, en su caso, en el Contrato para la prestación de servicios de certificados suscrito con la ECIBCE.

5.2.1.4. Obligaciones del Suscriptor del Certificado de Firma Electrónica

- Conocer y cumplir en todo momento con las leyes, normas y regulaciones emitidas por Autoridades, Organismos de Control, el Banco Central del Ecuador y la ECIBCE en su DPC y las correspondientes Políticas de Certificados. Las cuales se encuentran publicadas en el Portal web de la ECIBCE.

- Comunicar a la ECIBCE cualquier modificación o variación de los datos que se aportaron para obtener el Certificado de Firma Electrónica. En especial, revocar y obtener un nuevo certificado de firma electrónica en casos excepcionales como es el cambio de número de identificación o nombres, que puedan dar lugar a su identificación inexacta.
- Verificar, a través de la Lista de Certificados Revocados (CRL) o consulta en línea de estado de certificados, el estado de los Certificados de firma electrónica.
- Proteger, mantener la debida custodia y conservar el medio de almacenamiento del certificado de firma electrónica.
- Reportar, solicitar la revocatoria y/o revocar inmediatamente (según el mecanismo con el que cuente) el certificado de firma electrónica en caso de compromiso de la clave privada, pérdida o robo del contenedor de firma electrónica.
- Responder por el uso del Certificado de Firma Electrónica y de las consecuencias que se deriven de su utilización. En todo momento, el certificado digital de firma electrónica otorgado garantiza la autenticidad, integridad, no repudio y confidencialidad.
- Solicitar una nueva emisión del Certificado de firma electrónica a la ECIBCE y/o recuperación del certificado emitido en archivo, token u otro contenedor o desbloqueo del Token, si este lo permite, en caso de olvido de la contraseña de protección de la clave privada de protección del Certificado de Firma Electrónica o inutilización de datos del soporte del certificado, según corresponda.
- Solicitar la revocatoria o revocar el certificado digital de firma electrónica en caso de olvido de clave; y solicitar la emisión de un nuevo certificado.
- Cumplir con lo establecido en el artículo 17 de la Ley de Comercio Electrónico, Firmas Electrónicas y Mensaje de Datos:

"Art. 17.- Obligaciones del titular de la firma electrónica.- El titular de la firma electrónica deberá:

- a) Cumplir con las obligaciones derivadas del uso de la firma electrónica;*
- b) Actuar con la debida diligencia y tomar las medidas de seguridad necesarias, para mantener la firma electrónica bajo su estricto control y evitar toda utilización no autorizada;*
- c) Notificar por cualquier medio a las personas vinculadas, cuando exista el riesgo de que su firma sea controlada por terceros no autorizados y utilizada indebidamente;*
- d) Verificar la exactitud de sus declaraciones;*
- e) Responder por las obligaciones derivadas del uso no autorizado de su firma, cuando no hubiere obrado con la debida diligencia para impedir su utilización, salvo que el destinatario conociere de la inseguridad de la firma electrónica o no hubiere actuado con la debida diligencia;*

- f) Notificar a la entidad de certificación de información los riesgos sobre su firma y solicitar oportunamente la cancelación de los certificados; y,*
- g) Las demás señaladas en la Ley y sus reglamentos."*

5.2.1.5. Obligaciones y Responsabilidades de los Usuarios

Los usuarios que confíen y usen los Certificados emitidos por la ECIBCE deberán verificar la validez de las firmas generadas por los Suscriptores. En el supuesto de que los Usuarios no verificaran las firmas a través de la CRL (Lista de Certificados revocados) u OCSP, la ECIBCE no se hace responsable del uso y confianza que los Usuarios hagan de estos certificados y firmas electrónicas.

Los servicios CRL y OCSP se encuentran expuestos a los usuarios a través del Portal web de la ECIBCE.

5.2.1.5.1. Confianza en los Certificados

Toda persona tendrá derecho a confiar en un Certificado de la ECIBCE, en la medida en que sea razonable hacerlo, acorde a las seguridades ofrecidas y verificadas.

Para determinar si es razonable confiar en el certificado, deberá tenerse en cuenta, en su caso, lo siguiente:

- Toda restricción a que esté sujeto el certificado;
- Si la parte que confía ha adoptado las medidas adecuadas para determinar la fiabilidad del certificado;
- Las políticas y procedimientos que rigen la actividad de la ECIBCE en relación con las diferentes Firmas Electrónicas realizadas con los tipos de certificados emitidos por la ECIBCE, políticas y procedimientos que se especifican en esta DPC y en las PCs de la ECIBCE para cada tipo de certificado.

Los usuarios del servicio de certificación de la ECIBCE se obligan a conocer y aceptar los términos, condiciones y límites contenidos en esta DPC y en las PCs específicas de su certificado.

5.2.2. Responsabilidades

5.2.2.1. Responsabilidades de la Autoridad de Certificación (AC)

Las responsabilidades de la Autoridad de Certificación (AC) o Entidad de Certificación de Información son las siguientes:

- Garantizar el cumplimiento de las responsabilidades y obligaciones descritas en esta DPC, la Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos y su Reglamento General, así como la Acreditación emitida por el Organismo de Control.

- La ECIBCE, única y exclusivamente, responderá por los daños y perjuicios que causen a cualquier persona, cuando incumpla sus obligaciones legales derivadas de la legislación vigente en la República del Ecuador o cuando actúe con negligencia en la prestación de servicios de certificación.
- La ECIBCE no será responsable de los daños derivados de o relacionados con la no ejecución o ejecución defectuosa de las obligaciones a cargo del Solicitante, Suscriptor y/o Usuario.
- La ECIBCE no será responsable de la utilización negligente o dolosa de los Certificados digitales, ni de las claves.
- La ECIBCE no será responsable de los daños y perjuicios que se deriven de actuaciones negligentes o dolosas por parte de terceros con relación a los certificados digitales por ella emitidos en favor de un determinado suscriptor.
- La ECIBCE no será responsable de las eventuales inexactitudes en el Certificado digital que resulten de la información facilitada por el Solicitante o Suscriptor del certificado, a condición de haber actuado siempre con la máxima diligencia exigible.
- La ECIBCE no será responsable de los daños que se deriven de aquellas operaciones en que se hayan incumplido las limitaciones de uso que se señalan en las Políticas de Certificación correspondientes a cada tipo de certificado.
- La ECIBCE no asumirá responsabilidad alguna por la no ejecución o el retraso en la ejecución de cualquiera de las obligaciones en virtud de la presente DPC. Si tal falta de ejecución o retraso resultara o fuera consecuencia de fuerza mayor, caso fortuito o, en general, cualquier circunstancia sobre la que la ECIBCE no pueda tener un control razonable.
- La ECIBCE no será responsable del contenido de aquellos documentos digitales firmados electrónicamente. Ni la ECIBCE ni sus Autoridades de Registro o Terceros Vinculados serán responsables en ningún caso por los daños causados por el empleo de sus servicios de certificación pública.
- No se admitirán responsabilidades frente a terceros, que se basen en un certificado digital emitido por la ECIBCE, si aquellos terceros tuviesen indicios o constancia de que el certificado o su clave pública asociada han sido objeto de manipulación o mal uso. Tales indicios incluyen, aunque no se limitan a: los contenidos del certificado, la información incorporada al certificado por referencia, así como los contenidos de esta DPC y la Lista de Certificados Revocados publicada por la ECIBCE.

5.2.2.2. Responsabilidades de la AR

- La AR responderá por las funciones que le correspondan conforme a esta DPC y, en especial, asumirá toda la responsabilidad por la correcta identificación y validación del

Solicitante / Suscriptor, con las mismas limitaciones que se establecen en el apartado anterior con relación a la ECIBCE.

- La AR, responderá ante la ECIBCE por los daños y perjuicios que pudieran derivarse de la ejecución de esas funciones concertadas de manera negligente o en forma distinta a la contemplada en la presente DPC y en las PCs emitidas para cada tipo de Certificado.
- No obstante, la AR no se hace responsable, en ningún caso, de la identidad o identificación del solicitante y/o suscriptor en el supuesto de falsificación de la documentación u otros datos aportados, por él mismo o por tercero que le suplantare.

5.2.2.3. Responsabilidades del Suscriptor

- El Suscriptor será responsable por los daños y perjuicios causados por el incumplimiento de sus respectivas obligaciones enumeradas en esta DPC.
- El Suscriptor será responsable del cumplimiento de todas aquellas obligaciones impuestas por la presente DPC, las PC de cada tipo de Certificado, contrato de prestación de servicios suscrito y por la normativa vigente en materia de prestación de servicios de certificación.
- El Suscriptor del certificado será responsable por los daños y perjuicios causados por el incumplimiento de sus respectivas obligaciones enumeradas en esta DPC.
- El Suscriptor se compromete a indemnizar a la ECIBCE por los daños o perjuicios que puedan ocasionar cualquier acto u omisión culposa o dolosa por su parte, asumiendo igualmente los costos procesales en que la ECIBCE pudiera incurrir por esta causa, incluyendo los honorarios profesionales de Abogados y Procuradores.
- El suscriptor indemnizará y mantendrá indemne a la ECIBCE por cualquier daño que ésta pudiera sufrir por el incumplimiento total, parcial o defectuoso de las obligaciones asumidas y en base a toda reclamación dirigida contra ella por cualquier tercero con el que el suscriptor hubiera contratado.

5.2.2.4. Responsabilidades del Usuario

- El Usuario será responsable por los daños y perjuicios causados por el incumplimiento de sus respectivas obligaciones enumeradas en esta DPC.
- El Usuario será responsable del cumplimiento de todas aquellas obligaciones impuestas por la presente DPC, las PC de cada tipo de Certificado, y por la normativa vigente en materia de prestación de servicios de certificación.
- El Usuario será responsable por los daños y perjuicios causados por el incumplimiento de sus respectivas obligaciones enumeradas en esta DPC.
- En todo caso, el Usuario asumirá toda la responsabilidad y riesgos derivados de la aceptación de un Certificado digital y firma electrónica del mensaje de datos, sin haber

observado las obligaciones recogidas en la DPC y, en su caso, en las PC específicas de cada certificado, garantizando la plena indemnidad de la ECIBCE por dicho concepto.

5.2.3. Políticas de Manejo de los Certificados de Firma Electrónica de la ECIBCE

- Los datos que son almacenados en el certificado no contendrán tildes, ñ, ni diéresis.
- El suscriptor podrá hacer uso del certificado de Firma Electrónica según lo establecido en la política del certificado, en el contrato de prestación de servicios que suscriba con la ECIBCE y en esta DPC.
- Se considerará que se hace uso indebido de un Certificado, cuando éste sea utilizado para realizar operaciones no autorizadas según las Políticas de Certificados aplicables a cada tipo de Certificado, y los Contratos de la ECIBCE con sus suscriptores, consecuencia de esto la ECIBCE podrá revocar el certificado y dar por terminado el contrato.
- El certificado emitido en cualquier tipo de contenedor (archivo en formato PKCS#12 o PFX, roaming, dispositivo móvil smartphone o tablet, dispositivo TOKEN, etc.) deberá ser custodiado por el suscriptor y será responsabilidad total de éste el manejo y uso del certificado digital, incluido su clave privada para firma de mensajes de datos o documentos.
- Los usos autorizados de los certificados emitidos por la ECIBCE, están especificados en las Políticas de Certificados de cada tipo de certificado.
- Si el certificado del suscriptor durante el período de vigencia se encontrara comprometido, es decir, su clave privada y contraseña no están bajo el control del suscriptor, deberá iniciar el procedimiento de revocación como se lo menciona en esta DPC y en las Políticas de Certificación.
- El certificado de firma electrónica emitido por la ECIBCE al suscriptor, deberá ser utilizado tal y como es suministrado. Queda prohibida cualquier alteración del certificado por parte del usuario.
- Los certificados de firma electrónica no podrán ser utilizados para acciones ilícitas, de acuerdo a lo establecido en la legislación ecuatoriana.
- La firma electrónica, tecnológica y legalmente, ofrece las siguientes garantías:
 - Autenticidad. La información del documento y su firma electrónica, corresponden indubitavelmente con la persona que ha firmado.
 - Integridad.- La información contenida en el documento electrónico, no ha sido modificada o alterada luego de su firma.
 - No repudio.- La persona que ha firmado electrónicamente no puede negar su autoría.

- Confidencialidad.- Permite el acceso solo a las personas autorizadas y ofrece seguridad recíproca entre las partes.

IMPORTANTE

El sistema de cifrado, mediante el uso de claves públicas y privadas, es de total responsabilidad del usuario. Cabe señalar que la ECIBCE no guarda copia de seguridad de las claves privadas ni contraseñas del usuario.

Sin embargo, el uso de claves públicas contenidas en un certificado podría ser utilizado para CIFRADO DE DATOS, por lo que el usuario que utilice la clave pública para cifrar datos, únicamente el destinatario podrá descifrar con su clave privada. En caso de olvido de la clave, el mensaje simplemente no se podrá descifrar por ningún medio.

La ECIBCE no asume ninguna responsabilidad en lo relacionado a cifrado de datos.

5.2.4. Interpretación y Ejecución

5.2.4.1. Ley Aplicable

El presente documento y las Prácticas de Certificación específicas para cada tipo de Certificado se regirán por la Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos, con arreglo a la cual deberá ser interpretado su contenido.

5.2.4.2. Transferencia de certificados y Notificaciones

La ECIBCE no podrá ceder o transferir total ni parcialmente la Acreditación, ni los derechos y deberes derivados de la misma, conforme el art. 18 del Reglamento a la Ley de Comercio Electrónico y artículo 8 Resolución ARCOTEL-2018-0902. De acuerdo a lo establecido en el artículo 13 del Reglamento a la Ley de Comercio Electrónico “(...) En caso de que las actividades de certificación vayan a cesar, la entidad de certificación deberá notificar con por lo menos noventa (90) días de anticipación a los usuarios de los certificados de firma electrónica y a los organismos de regulación control sobre la terminación de sus actividades. La cesión de certificados de firma electrónica de una entidad de certificación a otra, contará con la autorización expresa del titular del certificado. La entidad de certificación que asuma los certificados deberá cumplir con los mismos requisitos tecnológicos exigidos a las entidades de certificación por la Ley 67 y este reglamento.”

Ante esta hipotética cesión de certificados, la ECIBCE realizará todas las actividades necesarias conforme la citada Ley y su Reglamento, antes de transferir la gestión completa de los certificados, que continúen en vigencia a la fecha en que se produzca la misma, a otro prestador de servicios de certificación Acreditado o, en caso contrario, extinguir la vigencia de los certificados. Para la consecución de estos objetivos, se establecen las siguientes medidas:

- 1) Comunicará al Organismo de Control y con una antelación mínima de tres (3) meses la cesación de actividades de certificación y terminación de sus actividades, informando al mismo tiempo sobre todas las características del Prestador de Servicios de Certificación Acreditado, al que se propone la cesión de los certificados.
- 2) La ARCOTEL deberá autorizar oficialmente la cesión que asume la otra Entidad de Certificación de Información debidamente Acreditada, garantizando que no se afecten los derechos del titular del certificado.
- 3) Esta DPC seguirá siendo el documento que regule las relaciones entre las partes, mientras no se cree un nuevo documento por escrito.
- 4) Recabar el consentimiento expreso de los suscriptores que tengan en ese momento certificados que estén en vigor para la transferencia de la gestión de los certificados. En caso de no contar con el consentimiento de los suscriptores se procederá con la revocatoria de los certificados correspondientes.
- 5) Proceder, en caso de no haberse podido llevar a cabo transferencia de derechos y obligaciones a otra entidad, a la revocación de todos los Certificados una vez transcurrido el plazo de dos (2) meses desde la comunicación.
- 6) Indemnizar adecuadamente a aquellos Suscriptores que lo soliciten cuando sus Certificados sean revocados con anterioridad al periodo previsto de vigencia, pactándose como tope para la indemnización el costo efectivo del servicio, descontando a prorrata el costo por los días transcurridos desde el inicio del contrato hasta la fecha de revocación.
- 7) Informará a las administraciones competentes, con la antelación indicada, la subrogación de su actividad y el destino que se vaya a dar a los certificados, especificando en su caso si se va a transferir la gestión y a quien.
- 8) Con carácter previo al cese definitivo de la actividad, comunicará a la administración competente la información relativa a los certificados emitidos al público cuya vigencia haya sido extinguida para que se haga cargo de su custodia.
- 9) Cualquier otra obligación de conformidad a lo estipulado en la Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos y su Reglamento, y otras normativas.

5.2.5. Procedimiento de Resolución de Conflictos

Las diferencias que se presenten entre las partes con ocasión de este Servicio, durante su ejecución o por su interpretación serán resueltas en primera instancia directamente entre el Usuario y la ECIBCE.

De no existir dicho acuerdo, podrán someter la controversia al proceso de mediación como un sistema alternativo de solución de conflictos reconocido constitucionalmente, para lo cual las partes estipulan acudir al Centro de Mediación de la Procuraduría General del Estado.

El proceso de mediación se sujetará a la Ley de Arbitraje y Mediación y al Reglamento de Funcionamiento del Centro de Mediación de la Procuraduría General del Estado.

Si se llegare a firmar un acta de acuerdo total, la misma tendrá efecto de sentencia ejecutoriada y cosa juzgada y su ejecución será del mismo modo que las sentencias de última instancia siguiendo la vía de apremio, conforme lo dispone el Art. 47 de la Ley de Arbitraje y Mediación.

En el caso de no existir acuerdo las partes suscribirán la respectiva acta de imposibilidad de acuerdo, y la controversia se ventilará ante el Tribunal Distrital de lo Contencioso Administrativo competente.

En el caso de suscribirse actas de acuerdo parcial, las mismas tendrán efecto de cosa juzgada sobre los asuntos acordados; y para el caso de aspectos sobre los cuales no se acuerde, éstos serán resueltos ante el Tribunal Distrital de lo Contencioso Administrativo competente.

La legislación aplicable es la ecuatoriana.

5.2.6. Tarifas de Servicios de Certificación Electrónica

Las tarifas vigentes por la emisión, renovación y recuperación por olvido de clave de Certificados digitales y otros servicios de certificación electrónica, serán puestas en conocimiento de los Solicitantes, a través del Portal web www.eci.bce.ec de la Entidad de Certificación de Información. Las tarifas se establecen mediante resolución administrativa aprobada por la Gerencia General del Banco Central del Ecuador.

5.2.7. Publicación y Custodia

5.2.7.1. Publicación de Información de la AC

El contenido de esta DPC, así como de toda la información que se publique, estará disponible en la dirección web: <http://www.eci.bce.ec>, sección Marco Normativo y los originales estarán custodiados en las oficinas de la ECIBCE o de forma digital.

5.2.8. Confidencialidad y Protección de Datos

5.2.8.1. Confidencialidad de las Claves de Firma Electrónica

La ECIBCE garantiza la confidencialidad frente a terceros durante el proceso de generación de las claves privadas de firma electrónica, que proporciona a sus suscriptores o que las Autoridades Certificadoras Subordinadas o de Segundo Nivel encadenadas con la ECIBCE proporcionan a sus suscriptores. Los procedimientos utilizados en la PKI para la generación de claves cumplen con estándares internacionales de seguridad. Así mismo, una vez generadas y entregadas las claves privadas, la ECIBCE no almacena, copia o conserva ningún tipo de información que pueda reconstruir dichas claves.

5.2.8.2. Confidencialidad en la Prestación de Servicios de Certificación

Tanto la ECIBCE como las AR o terceros vinculados, mantendrán la más estricta confidencialidad de toda información suministrada por los Solicitantes y Suscriptores de Certificados, siempre que la publicación o comunicación a terceros de dicha información no sea necesaria para la correcta prestación de los servicios de certificación. La ECIBCE solicitará la autorización de Solicitantes y Suscriptores cuando precise utilizar los datos para otros fines, a excepción de información que solicite la ARCOTEL, como organismo de control, la Fiscalía General del Estado o en cumplimiento de orden judicial.

5.2.9. Protección de Datos

A los efectos de lo dispuesto en la normativa sobre tratamiento de datos de carácter personal, se informa al Suscriptor/Solicitante de la existencia de un archivo automatizado de datos de carácter personal creado y/u obtenido a través o mediante el uso de plataformas de interoperabilidad gubernamental; y, bajo la responsabilidad de la ECIBCE y/o su Tercero Vinculado, con la finalidad de servir a los usos previstos en esta DPC o cualquier otro relacionado con los servicios de certificación. El Suscriptor/Solicitante consiente expresamente la cesión de sus datos de carácter personal contenidos en dicho archivo, en la medida en que sea necesaria para llevar a cabo las operaciones o procedimientos previstos en esta DPC.

El responsable del archivo, se compromete a poner los medios a su alcance para evitar la alteración, pérdida, tratamiento o acceso no autorizado a los datos de carácter personal contenidos en el archivo. Cualquier otra utilización de estos datos requerirá consentimiento previo del Suscriptor/Solicitante. Asimismo, se informa sobre el derecho que asiste al Suscriptor para acceder, modificar o rectificar sus datos de carácter personal, en los términos recogidos por la normativa sobre tratamiento de datos de carácter personal.

La información suministrada por el Solicitante/Suscriptor, es almacenada por la ECIBCE en formato electrónico o físico, de tal manera que en caso de requerir datos que necesiten ser convalidados, se pueda tener acceso a dichos documentos.

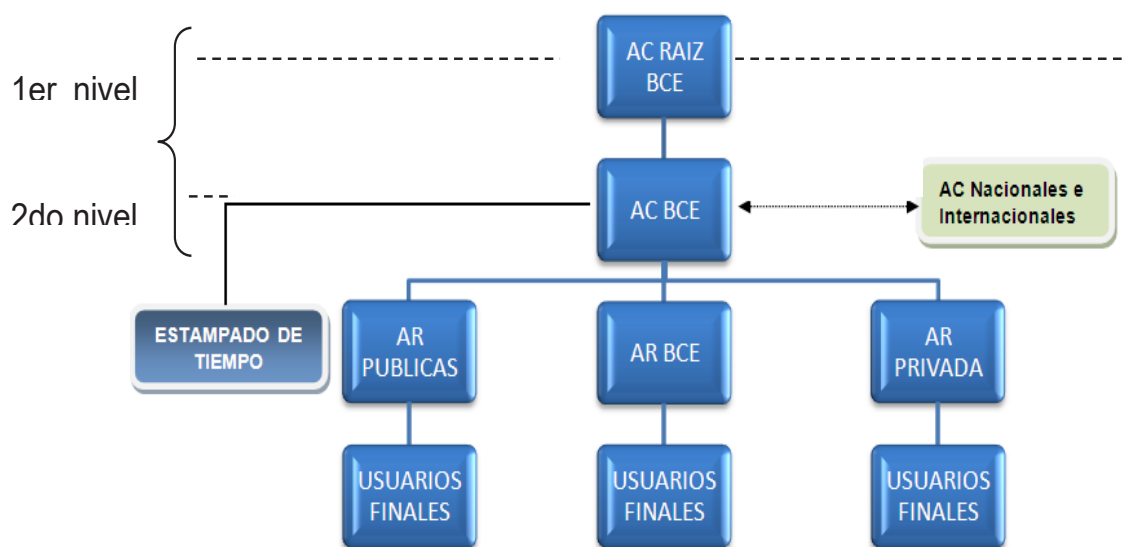
5.2.10. Derechos de Propiedad Intelectual

La ECIBCE es titular de todos los derechos de propiedad intelectual que puedan derivarse del sistema de certificación electrónica que regula esta DPC. Se prohíbe, por tanto, cualquier acto de reproducción, distribución, comunicación pública y transformación de cualquiera de los elementos que son titularidad exclusiva de la ECIBCE, sin la autorización expresa por su parte. No obstante, no necesitará autorización de la ECIBCE para la reproducción del datos o información del Certificado, cuando la misma sea necesaria para la utilización del mismo por parte del usuario legítimo y con arreglo a la finalidad de éste, de acuerdo con los términos de

esta DPC, la respectiva PC del certificado y, en su caso, en el contrato de prestación de servicios suscrito con la ECIBCE.

5.3. GESTIÓN DE CLAVES

La ECIBCE ha definido su jerarquía de Infraestructura de Clave Pública bajo la RFC 3280 donde básicamente contempla una AC RAIZ auto firmada, una AC subordinada, Autoridades de Registro (terceros vinculados) y Usuario Final.



Jerarquía Entidad de Certificación del Banco Central del Ecuador

Un primer nivel en el que se ubica la AC o CA RAIZ de la ECIBCE que representa el punto de confianza de todo el sistema y que permitirá, que todas las personas naturales y jurídicas, reconozcan la eficacia de los certificados de la ECIBCE para firma electrónica.

Un segundo nivel, constituido por la AC o CA Subordinadas de la ECIBCE, que emitirá los certificados digitales de firma electrónica de los suscriptores/usuario final y estampado de tiempo. En este nivel se pueden agregar otras AC, de esta forma la ECIBCE contará con diferentes AC Subordinadas.

5.3.1. Del Certificado de la AC Raíz y AC Subordinada de la ECIBCE

Las claves de la AC RAIZ y AC Subordinada de la ECIBCE son custodiadas en un ambiente seguro, bajo estándares de seguridad físicos como lógicos. El acceso a esas claves sólo se permite a personas debidamente autorizadas por la ECIBCE.

5.3.1.1. Generación del Par de Claves

Los pares de claves de la AC Raíz y AC Subordinadas del Banco Central del Ecuador se generan en módulos de hardware criptográficos “HSM – Hardware Security Module” que cumplen los requisitos establecidos en un perfil de protección de dispositivo seguro para Autoridad de Certificación de acuerdo con Common Criteria y FIPS 140-2 Nivel 3 o superior nivel de seguridad.

5.3.1.2. Protocolo de Generación del Par de Claves

La ECIBCE cuenta con un documento aprobado por la Gerencia General (Autoridad de Política) donde se detalla el procedimiento de generación de la clave raíz y claves subordinadas para la Autoridad de Certificación del Banco Central del Ecuador de acuerdo a la norma ISO 21188.

5.3.1.3. Entrega de Clave Pública de la AC Raíz y AC Subordinadas a los Usuarios Finales

Las claves públicas de la AC Raíz y AC Subordinadas de la cadena de certificación de la ECIBCE se pueden descargar del portal web <https://www.eci.bce.ec>, sección "Centro de Descargas".

5.3.1.4. Tamaño de las Claves

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 algoritmos actualizados como SHA2 de 256 bits y recomendados por el NIST.

El período de validez de las claves de la AC RAIZ es como máximo de veinte (20) años.

El periodo de validez de las claves de las AC Subordinadas es como máximo de diez (10) años.

5.3.1.5. Protección de Clave Privada de la AC Raíz y AC Subordinada de la ECIBCE

5.3.1.5.1. Control Multipersona de la Clave Privada

La clave privada de la AC Raíz y AC Subordinadas, se encuentra bajo control multipersona. Es decir, esta clave se activa mediante la inicialización del software de AC por medio de una combinación de operadores de la AC, administradores del HSM y usuarios de Sistema Operativo, debidamente autorizados. Éste es el único método de activación de dicha clave privada.

“Control multipersona: control por más de una persona, normalmente por un subconjunto ‘m’ de un total de ‘n’ personas. De esta forma, se garantiza que nadie tenga el control de forma individual de las actuaciones críticas, a la vez que se facilita la disponibilidad de las personas necesarias.”

5.3.1.5.2. Copia de Seguridad de la Clave Privada

Las copias o backups de las claves privadas de la AC RAIZ y AC Subordinada de la ECIBCE son almacenadas en dispositivos criptográficos seguros "TOKENs Backup."

Los TOKEN Backups custodian un respaldo de la clave privada y únicamente podrá ser accedida bajo el esquema multipersona, para la exportación y/o activación de la misma.

Contenido del Certificado de la AC RAÍZ de la ECIBCE

Contenido del Certificado de la AC RAÍZ de la ECIBCE		
Campo	Descripción	Valor
Versión	Versión del Certificado estándar X509	V3
Serial Number	Número que identifica unívocamente al certificado	4e 3f fa 6d
Algoritmo de firma	Algoritmo utilizado por la ECIBCE para firmar el certificado	sha256RSA
Emisor (issuer)	CN	AUTORIDAD DE CERTIFICACIÓN RAÍZ DEL BANCO CENTRAL DEL ECUADOR
	L	QUITO
	OU	ENTIDAD DE CERTIFICACIÓN DE INFORMACIÓN-ECIBCE
	O	BANCO CENTRAL DEL ECUADOR
	C	EC
Válido desde	Fecha y hora UTC desde que es válido el certificado	Lunes, 08 de agosto de 2011
Válido hasta	Fecha y hora UTC hasta la cual es válido el certificado	Viernes, 08 de agosto de 2031
Asunto	CN	AUTORIDAD DE CERTIFICACIÓN RAÍZ BANCO CENTRAL DEL ECUADOR
	L	QUITO
	OU	ENTIDAD DE CERTIFICACIÓN DE INFORMACIÓN-ECIBCE
	O	BANCO CENTRAL DEL ECUADOR
	C	EC
Clave pública	Clave pública de la AC RAÍZ de la ECIBCE	30 82 02 0a 02 82 02 01 00 bc 3d c0 7e c3 80 53 11 de 41 d4 a7 bd 96 a6 e8 35 37 c2 56 15 1b 61 9e 1a b1 31 6c 4e 5d 59 c6 a1 86 c6 b1 d5 53 6b 27 17 49 e5 67 5a

Contenido del Certificado de la AC RAÍZ de la ECIBCE		
Campo	Descripción	Valor
		dd 37 01 90 c6 c3 cc 7b 14 d8 77 03 61 e1 f6 fb 4e 64 69 c5 08 e5 89 67 20 ea 17 92 a2 18 73 7a 26 2c b5 98 00 f8 a8 08 05 82 15 82 87 bf 0e 04 ed 7d 4e 12 37 3c 07 e5 7a f3 30 aa 75 85 e4 32 6c a8 17 55 f2 5a af 3a 1f 0b e4 35 f9 e0 f0 d8 72 cd b3 5e 50 48 ef a8 73 fd 87 b8 05 72 35 74 c4 a6 94 a6 c0 55 a8 81 30 c1 be 61 ef ec cc 02 f8 45 00 99 36 9c a2 eb 99 db 81 72 b3 b5 bb d6 8f 02 62 24 86 d6 28 d0 fd 0a ee 34 fb 06 7a b6 6f 8e 71 32 b2 35 07 e1 bd d4 9f a9 16 7b b5 0b f6 2c 3c 21 3e 8b 6e ce dc 92 e9 19 63 c8 cc 8d 7b 59 77 03 a8 56 0f f2 67 4b ae 60 1e 2e 3a 1f 45 a3 ad 1a ad 1f 93 9b aa 14 c4 c1 9b 33 38 f7 54 df 65 45 70 b8 54 b5 98 4f 42 9d 0c ef 85 9a d9 d5 f2 f5 df ac 0c 10 9d 23 d1 99 71 a6 3e 9f 36 8d 31 b3 c4 75 3e 65 16 0d 54 73 a9 2c 59 b5 af 8f 9b 9d 64 c0 61 ca 06 63 d4 fb 5a 58 58 e6 aa 96 5c 75 df 6f 67 6f 46 19 b3 ad 28 1e 9b c7 5e b6 60 66 8a e6 c1 a3 07 7f 39 59 50 d1 02 2e 94 ce 39 7e d0 2a 68 0c 98 cf ed 84 bd b5 9a d7 94 3b 38 81 ea 69 28 44 ed 85 4d 9c a6 4e f7 8d 87 e5 cc 17 85 15 ab ee c4 d1 c6 93 a7 15 36 01 6b ae 18 6d d1 7d 3f 78 c8 60 ab 41 a8 e0 d5 32 63 5d 60 fe be df dd 4a 5f d1 84 7b 3b 13 9a 72 30 db 2e 92 1b 37 1c de 1f 68 6d 70 3d 33 a7 24 b8 f3 94 d6 9c 19 da ae 30 61 80 ed 72 c1 09 91 43 f4 72 97 c6 6a bb b7 96 28 13 9f 93 ef a1 89 ba 89 35 f7 8b c0 46 37 b8 11 a8 21 36 d3 5e 90 62 5f 6b ba 53 ce 9b 44 61 c4 4b 40 a6 ea 6b 9d e7 11 2b 02 03 01 00 01
Directivas o Bases del Certificado	Identificador de Objetos según la normalización internacional de la IANA	1.3.6.1.4.1.37947.1.1 http://www.eci.bce.ec/autoridad-certificacion/declaracion-practicas-certificacion.pdf
Algoritmo de identificación	Algoritmo Hash que genera una síntesis de datos o huella digital para las firmas digitales	sha1
Huella digital	La síntesis o huella digital de los datos del certificado	38 3f 64 60 4b 56 49 7a 47 9e 15 13 84 33 96 4e 4c a9 dd f4

Contenido del Certificado de la AC RAÍZ de la ECIBCE		
Campo	Descripción	Valor
Uso de clave	Propósito para los cuales se debe utilizar el certificado	Firma de certificados, Firma CRL sin conexión, Firma de lista de revocación de certificados (CRL) (06),

Contenido del Certificado de la AC Subordinada de la ECIBCE

Contenido del Certificado de la AC SUBORDINADA de la ECIBCE		
Campo	Descripción	Valor
Versión	Versión del Certificado estándar X509	V3
Serial Number	Número que identifica unívocamente al certificado	4e 3f fa 9e
Algoritmo de firma	Algoritmo utilizado por la ECIBCE para firmar el certificado	sha256RSA
Emisor (issuer)	CN	AUTORIDAD DE CERTIFICACIÓN RAÍZ DEL BANCO CENTRAL DEL ECUADOR
	L	QUITO
	OU	ENTIDAD DE CERTIFICACIÓN DE INFORMACIÓN-ECIBCE
	O	BANCO CENTRAL DEL ECUADOR
	C	EC
Válido desde	Fecha y hora UTC desde que es válido el certificado	Lunes, 08 de Agosto de 2011
Válido hasta	Fecha y hora UTC hasta la cual es válido el certificado	Domingo, 08 de Agosto de 2021
Asunto	CN	AC BANCO CENTRAL DEL ECUADOR
	L	QUITO
	OU	ENTIDAD DE CERTIFICACIÓN DE INFORMACIÓN-ECIBCE
	O	BANCO CENTRAL DEL ECUADOR
	C	EC
Clave pública	Clave pública de la AC Subordinada de la ECIBCE	30 82 02 0a 02 82 02 01 00 ae cd 60 d3 e6 4d 48 e1 37 47 89 06 f3 35 b9 66 25 32 01 e5 a1 76 01 74 78 98 30 f0 55 1f 5e ef 54 11 61 e0 d1 d2 ec 99 a1 9d b1 f8 35 7c 73 6f ff 03 f6 c9 72 cc 16 f0 b5 7a 0a e3 2d 8c 44 12 85 ab 09 7a e3 14 82 41 07 17 02 dd f9 d2 a9 ba d3 91 41

Contenido del Certificado de la AC SUBORDINADA de la ECIBCE		
Campo	Descripción	Valor
		8d b8 be 63 ae 30 3d 29 fa f6 08 ed 20 7a f0 25 0f 34 ae ac 1d b1 46 c6 96 c3 d9 15 8c 00 68 74 e0 66 c1 4d b1 89 02 f2 81 9b be 98 ea 4f 48 a2 c0 43 af 6f e9 7f ba 8b bb 2e 95 ad 1d a9 65 42 93 15 a2 72 c6 7d 10 2f c5 7c 83 f8 9b c6 99 a1 60 9f 09 4e 4c 37 86 ba 5d ba ee 54 12 d2 a4 e3 5f ed b6 1e 13 97 f6 c7 83 5f f3 0d ff db 2d 7b a9 33 1e 70 7a f1 f5 89 11 1a 17 70 fd b4 57 2f 4a 2f e1 3a 05 05 6e 33 7a db b7 43 14 d3 6f e9 fd f8 1c cf c9 f6 02 f8 96 08 ce f8 1b 4b 94 eb 3e 55 04 c9 de 8c 84 4a 84 4a a0 43 ec 30 29 2a d4 f0 bd 6b c2 c7 ea 21 1d 84 be a0 28 23 4f 33 34 13 98 20 3c 69 46 fd 56 1a 42 bd a8 a4 e5 4a 27 c7 aa 2c 9d b2 60 32 cd ca 79 48 2b 70 cc 3e dc 64 9f 0b ea 10 a0 c7 08 d7 1b 02 23 d5 47 80 7f b8 74 09 50 c8 20 21 75 39 13 83 72 c1 c9 61 8c db c7 39 bb 02 08 22 2d 29 1b f7 b2 89 0e 90 61 c9 37 ab 22 6f c5 3e 34 1e 8e 9c db 70 00 77 f4 ff 36 8d 27 48 3b a7 a2 84 e7 14 3e ca f6 48 69 78 79 9a 37 32 45 58 1a 41 bc 80 9c 24 ee 9c 60 39 cf 18 80 26 07 f1 6d fd 4e 9d 39 2a ad 7f bc c9 95 db e2 4f f8 01 21 c4 a0 a9 0f ba be 0a 00 4f 35 36 0d 5d 38 31 13 fc f2 0c 99 ab e6 91 25 98 e7 4b 3c f4 59 04 03 fe dc fc 91 16 97 88 b6 73 de 74 b9 cf b3 7a c5 47 6f e1 a2 53 67 f1 e3 f3 64 54 a3 f4 46 9b 44 d2 fe 24 d4 3c ad 46 56 c6 36 d3 c7 19 c4 75 21 0e 2d 6c c5 02 03 01 00 01
Directivas o Bases del Certificado	Identificador de objetos según la normalización internacional de la IANA	1.3.6.1.4.1.37947.1.1 http://www.eci.bce.ec/autoridad-certificacion/declaracion-practicas-certificacion.pdf
Algoritmo de identificación	Algoritmo Hash que genera una síntesis de datos o huella digital para las firmas digitales	sha1
Huella digital	La síntesis o huella digital de los datos del certificado	be 20 b1 4c e6 47 2b c0 70 ce 5d 3f 51 46 ea d4 a2 f7 27 7e

Contenido del Certificado de la AC SUBORDINADA de la ECIBCE		
Campo	Descripción	Valor
Uso de clave	Propósito para los cuales se debe utilizar el certificado	Firma de certificados, Firma CRL sin conexión, Firma de lista de revocación de certificados (CRL) (06)

5.3.2. De Certificados de Usuario Final

En general, la ECIBCE seguirá una serie de estándares o normas a la hora de generar el par de claves para usuario final, como prestador de servicios de certificación. Estas normas o estándares son las siguientes:

- El tamaño de las claves será como mínimo de 2048 bits.
- El algoritmo utilizado para la generación de las claves es RSA.
- La generación de la función resumen (HASH) se realiza utilizando el algoritmo SHA2 de 256 bits o los recomendados por el NIST.
- El período de validez de las claves será el máximo establecido por la legislación vigente o lo establecido en la Política de certificado correspondiente desde que se emite o renueva el Certificado.

5.3.2.1. Generación del Par de Claves

Las claves de usuario final son generadas bajo estándares de seguridad internacional, que garantizan al usuario la seguridad en el uso de los certificados digitales.

Las claves públicas y privadas (no exportable) que son almacenadas en TOKEN en formato PKCS#11, para usuario final cumplen niveles de seguridad FIPS 2 Nivel 2 y 3, los mismos que custodiarán el certificado por el tiempo de vigencia. En el caso de TOKEN el acceso único será a través de un PIN (Personal Identification Number) o clave que el usuario exclusivamente conoce.

Las claves públicas y privadas que son almacenadas en archivo en formato PKCS#12, podrán ser exportables, de tal manera serán únicamente accedidas a través de un PIN (Personal Identification Number) o clave que el usuario exclusivamente conoce.

Nota: La ECIBCE se responsabiliza hasta la generación del certificado y entrega del mismo. Una vez entregado, el usuario será responsable del uso, custodia y manejo del certificado en archivo, TOKEN, roaming, HSM y contenedor celular.

Las claves que son almacenadas en HSM en formato PKCS#10, no son exportables, de tal manera serán únicamente accedidas a través de un PIN o clave que el usuario lo asigna.

Las claves que son almacenadas en servidor Roaming, podrán ser utilizadas, de tal manera serán únicamente accedidas a través de un identificador de usuario (ID) y PIN o clave que el usuario lo crea al momento de la emisión y que solo él la conoce.

Mayor información se describe en la política de cada tipo de certificado emitido por la ECIBCE.

5.4. SOLICITUD DE SERVICIOS DE CERTIFICACIÓN

5.4.1. Emisión de Certificados de Firma Electrónica

Este procedimiento se establece para los casos en que una persona desea solicitar la emisión de un certificado de firma electrónica. Con este fin el solicitante llenará la solicitud correspondiente al tipo de certificado requerido, disponible en el portal Web de la ECIBCE y subirá la documentación en formato electrónico de acuerdo al tipo de certificado.

La información suministrada será sometida a un proceso minucioso de verificación para comprobar fehacientemente la identidad de la persona que está solicitando la emisión del certificado. La ECIBCE directamente o a través de su Tercero Vinculado podrá brindar servicios en línea, operar con enlaces a plataformas de interoperabilidad gubernamental para obtener y/o comparar información o documentación del solicitante, además podrá incluir en el proceso de identificación sistemas de validación biométrica que cuente con certificaciones de calidad y/o que cumpla con estándares internacionalmente aceptados.

La ECIBCE directamente o a través de sus oficinas de atención al cliente o de un Tercero vinculado a la ECI, tendrá la potestad de aprobar o no la solicitud. Aprobada la solicitud, el solicitante efectuará el pago de la tarifa respectiva, de dicho pago será notificado.

Una vez realizado el pago, el solicitante podrá acudir a la ECIBCE o al Tercero vinculado, para que una vez que se identifique proceder a la emisión del certificado solicitado.

El solicitante/suscriptor se identificará ante la Autoridad de Registro de la ECIBCE con una cédula o pasaporte válidos y suficientemente claros y actualizados para permitir su inequívoca identificación; suscribirá de forma digital tanto la solicitud y el contrato de prestación de servicios y se le entregará el certificado emitido, para que proceda a ingresar su clave de seguridad.

Los certificados emitidos por la ECIBCE tienen un plazo de vigencia establecido en el propio certificado y siempre será acorde con la legislación vigente y la política del certificado.

Los requisitos previos, la forma de solicitar la emisión y el procedimiento de emisión de certificados serán los que se especifiquen en las PC de cada Certificado. Dichos requisitos podrán considerar las políticas contempladas en la Ley Orgánica para la Optimización y Eficiencia de Trámites Administrativos.

5.4.2. Emisión de Certificados para Servidor Seguro SSL

Este procedimiento se establece para los casos en que una empresa participante en el Sistema Nacional de Pagos del Banco Central del Ecuador, u otros, solicite la emisión de un certificado de servidor seguro SSL. Con este fin el solicitante llenará la solicitud/formulario correspondiente, disponible en el portal Web del BCE <https://www.bce.ec/index.php/component/k2/item/1241->

tr%C3%A1mites-persona-jur%C3%ADdica y adjuntará la documentación requerida para este tipo de certificado.

La información suministrada será sometida a un proceso minucioso de verificación. La ECIBCE tendrá la potestad de aprobar o no la solicitud. Aprobada la solicitud, el solicitante efectuará el pago de la tarifa respectiva.

Una vez realizado el pago, el solicitante procede a generar la clave privada del certificado digital y envía a la ECIBCE por correo electrónico la petición o request (CSR).

Una vez comprobado el pago, el certificado de clave pública en formato .cer (de acuerdo al procedimiento vigente) será enviado al solicitante.

Los requisitos previos, la forma de solicitar la emisión y el procedimiento de emisión de certificados serán los que se especifiquen en las PC de este Certificado.

Los certificados emitidos por la ECIBCE para este fin tienen un plazo de vigencia establecido en el propio certificado y siempre será acorde con la legislación vigente y la política del certificado.

5.5. REVOCACIÓN Y SUSPENSIÓN DE CERTIFICADOS

5.5.1. Supuestos de Revocación

Los Certificados deberán ser revocados cuando concurra alguna de las circunstancias siguientes:

- Solicitud voluntaria del Suscriptor del certificado.
- Olvido de clave (aplica una recuperación del certificado).
- Inutilización de datos del soporte del certificado (problemas con el medio donde se encuentra almacenado el certificado). [de ser el caso podría aplicar una recuperación del certificado].
- Fallecimiento del suscriptor, incapacidad sobrevenida, total o parcial, terminación de la representación o extinción de la persona jurídica representada.
- Cese en su actividad del suscriptor.
- Cese en su actividad del prestador de servicios de certificación, salvo que los certificados expedidos por aquel sean transferidos a otro prestador de servicios.
- Inexactitudes en los datos aportados por el suscriptor para la obtención del certificado, así como la concurrencia de circunstancias que provoquen que dichos datos, originalmente incluidos en el Certificado, no se adecuen a la realidad.
- Que se detecte que las claves privadas del Suscriptor o de la AC han sido comprometidas, bien porque concurren las causas de pérdida, robo, hurto, modificación, divulgación o revelación de las claves privadas, bien por cualquier otra circunstancia, incluidas las fortuitas, que indiquen el uso de las claves privadas por persona distinta al titular.

- Por incumplimiento por parte de la AR, AC o el Suscriptor de las obligaciones establecidas en esta DPC.
- Por la finalización del plazo del contrato de servicios.
- Por cualquier causa que razonablemente induzca a creer que el servicio de certificación haya sido comprometido hasta el punto que se ponga en duda la fiabilidad del Certificado.
- Por resolución judicial o administrativa que lo ordene.
- Por las causas que se establecen en los artículos 26, literal b) y artículo 37 literal b) de la Ley de Comercio Electrónico, Firmas Electrónicas y Mensaje de Datos.

"Art. 26.- Revocatoria del certificado de firma electrónica.- El certificado de firma electrónica podrá ser revocado por el Consejo Nacional de Telecomunicaciones, de conformidad con lo previsto en esta Ley, cuando:

- a) La entidad de certificación de información cese en sus actividades y los certificados vigentes no sean asumidos por otra entidad de certificación; y,*
- b) Se produzca la quiebra técnica de la entidad de certificación judicialmente declarada."*

"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."*
- Por la concurrencia de cualquier otra causa especificada en la presente DPC, o en las correspondientes PCs establecidas para cada tipo de Certificado.

5.5.1.1. Efectos de la Revocación

El efecto de la revocación del Certificado es la pérdida de fiabilidad del mismo, originando el cese permanente de la operatividad del Certificado conforme a los usos que le son propios y, en consecuencia, de la prestación de los servicios de certificación.

La revocación de un Certificado impide el uso legítimo del mismo por parte del Suscriptor.

La revocación del Certificado por causa no imputable al Suscriptor originará la emisión de un nuevo Certificado a favor del Suscriptor por el plazo equivalente al restante para concluir el período originario de validez del Certificado revocado o de ser el caso por un nuevo período a partir de la nueva emisión.

La revocación del Certificado tendrá como consecuencia la notificación a terceros de que un Certificado ha sido revocado, cuando se solicite la verificación del mismo.

5.5.2. Supuestos de Suspensión

El certificado podrá ser suspendido cuando existan indicios sobre la existencia de una causa de revocación.

5.5.3. Efectos y Límites de la Suspensión

El efecto de la suspensión de los Certificados es la pérdida de fiabilidad de los mismos, originando el cese temporal o definitivo de la operatividad del Certificado conforme a los usos que le son propios y, en consecuencia, de la prestación de los servicios de certificación. La suspensión de un Certificado impide el uso legítimo del mismo por parte del Suscriptor.

La suspensión del Certificado terminará por cualquiera de las siguientes causas:

- Por decisión de la AC de suspender el Certificado.
- Por decisión de la AC de levantar la suspensión del Certificado, una vez considerada la improcedencia de la revocación.
- Por la finalización anticipada del procedimiento de revocación.

5.5.4. Procedimiento de Suspensión y Revocación

Deberán solicitar la suspensión/revocación en cuanto tengan conocimiento de la concurrencia de alguna de las circunstancias contempladas en el apartado anterior:

- El Suscriptor del Certificado
- La AR, respecto a aquellos Certificados en cuya emisión haya participado.
- El representante legal de la persona jurídica de derecho público o privado relacionada con el certificado.

Asimismo, podrá solicitar la suspensión/revocación cualquier tercero con un interés legítimo en caso de que tenga conocimiento de la existencia de alguna de las siguientes causas:

- Pérdida del soporte del Certificado.
- Fallecimiento del signatario.
- Incapacidad sobrevenida, total o parcial.
- Inexactitudes en el certificado.

- Compromiso de la fiabilidad del Certificado.
- Compromiso de las claves.
- Cese del Representante Legal.
- Extinción de la persona jurídica.
- Revocación de la autorización de la entidad que conste en el Certificado.

En todo caso, la ECIBCE podrá iniciar de oficio el procedimiento de suspensión/revocación de Certificados, en cualquiera de los casos previstos en el apartado anterior.

La Autoridad judicial o administrativa podrá, en aquellos supuestos que marque la Ley, así como las demás disposiciones vigentes, instar a la ECIBCE a suspender/revocar el certificado.

5.5.4.1. Recepción de Solicitudes de Suspensión/Revocación

La solicitud de suspensión/revocación de Certificados de un tercero (al que se hace referencia en el segundo párrafo del numeral anterior 5.5.4) se podrá dirigir a la ECIBCE en la forma de comunicación escrita o con firma digital, o presentándose físicamente ante la ECIBCE.

El Solicitante/Suscriptor que solicite la suspensión/revocación deberá hacerlo mediante el formulario de revocación disponible en la página del portal Web de la ECIBCE www.eci.bce.ec y/o a través de aplicativos o plataforma en línea de Terceros Vinculados a la ECIBCE, que se ponga a disposición del público.

Cuando la persona que solicite la suspensión/revocación del certificado no sea el propio suscriptor, deberá ser solicitada por el Representante Legal, en caso de Persona Jurídica, y en caso de Persona Natural podrá gestionar de manera presencial o a través de una persona debidamente autorizada para validar el proceso.

5.5.4.2. Decisión de Suspender/Revocar

Una vez recibida y autenticada la solicitud de revocación, la ECIBCE procederá a tramitar la suspensión/revocación efectiva del Certificado. La decisión de suspender/revocar un Certificado corresponde a la ECIBCE.

Así también, la ECIBCE podrá habilitar a través de su portal web el proceso de autogestión de revocatorias de certificados, mediante el acceso de usuario y clave del suscriptor y que lo deberá confirmar en el sistema o mediante el ingreso del número de serie del certificado y código OTP recibido en el correo electrónico registrado por el suscriptor.

5.5.4.3. Comunicación y Publicación de la Suspensión/Revocación

La decisión de revocar el Certificado será comunicada por la ECIBCE al Suscriptor mediante correo electrónico.

Igualmente, se publicará la revocación del Certificado en la CRL. La publicación de las CRL's se realiza cada cuatro (4) horas o cada vez que se revoca un certificado, la vigencia de la CRL es de aproximadamente veinticinco (25) horas.

Su consulta se puede realizar vía web en:

http://www.eci.bce.ec/CRL/eci_bce_ec_crlfilecomb.crl

<http://ocsp.eci.bce.ec/ejbca/publicweb/status/ocsp>

<ldap://bceqldapsubp1.bce.ec/>

La revocación surtirá efecto frente a terceros a partir de su publicación por parte de la ECIBCE, salvo que la causa de revocación sea el cese de la actividad de prestación de servicios de certificación de la ECIBCE, en cuyo caso, la pérdida de eficacia tendrá lugar desde que la comunicación oficial de dicha extinción, se incluya en el servicio de consulta sobre vigencia de los certificados de la ECIBCE.

La información relativa al estado de la revocación estará disponible las 24 horas del día, los 7 días de la semana y los 365 días del año. En caso de fallo del sistema, servicio o cualquier otro evento, como fuerza mayor, que no esté bajo el control de la ECIBCE, ésta deberá realizar los esfuerzos que razonablemente estén a su alcance para restablecer el servicio en el menor tiempo posible.

5.6. RECUPERACIÓN DEL CERTIFICADO

5.6.1. Supuestos de Recuperación:

Los certificados cuya solicitud ha sido ingresada por alguna de las siguientes causas:

- Olvido de clave.
- Inutilización de datos del soporte del certificado (problemas con el medio donde se encuentra almacenado el certificado).

Serán recuperados, entendiéndose por recuperación a la emisión de un nuevo certificado de firma electrónica, por el tiempo restante de su vigencia, cuyos datos contenidos sean iguales al anteriormente generado con un nuevo número de serie de certificado digital; o el desbloqueo del dispositivo en los tipos soportados.

No obstante, por las causas antes citadas, el solicitante/suscriptor deberá optar por solicitar la revocatoria y una nueva emisión de certificado con nuevo plazo de vigencia, cuando por limitaciones técnicas o de infraestructura PKI o según el tipo de contenedor utilizado no sea posible la recuperación del certificado por el tiempo que resta de vigencia al inicialmente emitido.

5.6.2. Procedimiento de Recuperación

Se solicita la recuperación llenando el formulario correspondiente en el portal de Certificación Electrónica www.eci.bce.ec, en cuanto tenga conocimiento de la concurrencia de alguna de las circunstancias contempladas en el apartado anterior:

- El Solicitante/Suscriptor del Certificado
- La AR ECIBCE o Tercero Vinculado, respecto a aquellos Certificados en cuya emisión haya participado.

En todo caso, la ECIBCE podrá iniciar de oficio el procedimiento de recuperación de certificados, en cualquiera de los casos previstos en el apartado anterior.

5.7. CADUCIDAD DE CERTIFICADOS

El certificado caducará una vez concluido el período de vigencia del mismo. La caducidad producirá automáticamente la invalidez del Certificado, originando el cese permanente de su operatividad conforme a los usos que le son propios y, en consecuencia, de la prestación de los servicios de certificación. La caducidad de un Certificado impide el uso legítimo del mismo por parte del Suscriptor.

En todo caso, el usuario tiene pleno conocimiento de la fecha de emisión y de vigencia de su certificado digital de firma electrónica, a través del contrato suscrito con la AR o Tercero Vinculado, mediante consulta en el portal web de la ECIBCE y consulta del propio certificado en posesión del suscriptor.

5.8. RENOVACIÓN DE LOS SERVICIOS DE CERTIFICACIÓN

5.8.1. Renovación de Certificados

Este procedimiento se establece para los casos en que el certificado esté próximo a caducar y el suscriptor simplemente desee utilizar un certificado con las mismas características con el que venía utilizando.

En este caso, se le generarán nuevas claves; pero, únicamente se van a llevar a cabo unas medidas mínimas de comprobación, puesto que la información básica en el certificado originalmente emitido no ha variado.

Los certificados emitidos por la ECIBCE tienen un plazo de vigencia establecido en el propio certificado y siempre será acorde con la legislación vigente. Se podrá acudir a los trámites que se establecen en este documento para la renovación de los servicios de certificación si concurren las circunstancias recogidas en las PC de cada tipo de Certificado.

Los requisitos previos, la forma de solicitar la renovación y el procedimiento de renovación de certificados serán los que se especifiquen en las PC de cada Certificado.

5.9. EXTINCIÓN DE LA AC

La ECIBCE no podrá ceder o transferir total ni parcialmente la Acreditación, ni los derechos y deberes derivados de la misma, conforme el art. 18 del Reglamento a la Ley de Comercio Electrónico y artículo 8 Resolución ARCOTEL-2018-0902. De acuerdo a lo establecido en el artículo 13 del Reglamento a la Ley de Comercio Electrónico “(...) En caso de que las actividades de certificación vayan a cesar, la entidad de certificación deberá notificar con por lo menos noventa (90) días de anticipación a los usuarios de los certificados de firma electrónica y a los organismos de regulación control sobre la terminación de sus actividades. La cesión de certificados de firma electrónica de una entidad de certificación a otra, contará con la autorización expresa del titular del certificado. La entidad de certificación que asuma los certificados deberá cumplir con los mismos requisitos tecnológicos exigidos a las entidades de certificación por la Ley 67 y este reglamento.”

Ante un hipotético cese de la prestación de servicios de la ECIBCE, ésta realizará todas las gestiones necesarias para ceder, con el consentimiento expreso de los suscriptores, la gestión de los certificados que sigan vigentes en la fecha en que se produzca el cese, a otro prestador de servicios de certificación Acreditado que los asuma o, en caso contrario, extinguir la vigencia. Para la consecución de estos objetivos se establecen las siguientes medidas:

- Establecer, cuando ello fuera posible, un acuerdo con otro Prestador del Servicio de Certificación Acreditado, con el propósito de efectuar la cesión de certificados con la intención de continuar el servicio. Si se produce la cesión, esta DPC seguirá siendo el documento que establece las relaciones entre las partes mientras no se establezca un nuevo documento por escrito. Comunicará al Organismo de Control y con una antelación mínima de tres (3) meses el cese de la actividad, informando al mismo tiempo sobre todas las características del Prestador de Servicios de Certificación Acreditado al que se propone ceder los certificados.
- La ARCOTEL deberá autorizar oficialmente la cesión de certificados que asume la otra Entidad de Certificación de Información debidamente Acreditada.
- Recabar el consentimiento expreso de los suscriptores que tengan en ese momento certificados que estén vigentes para la transferencia de la gestión de los certificados.
- Proceder, en caso de no haberse podido llevar a cabo la transferencia de derechos y obligaciones a otra entidad Acreditada, a la revocación de todos los Certificados una vez transcurrido el plazo de dos (2) meses desde la comunicación.
- Indemnizar adecuadamente a aquellos Suscriptores que lo soliciten cuando sus Certificados sean revocados con anterioridad al plazo previsto de vigencia, pactándose como tope para la indemnización el costo efectivo del servicio, descontando a prorrata el costo por los días transcurridos desde el inicio del contrato hasta la fecha de revocatoria.

- Informar a los organismos competentes, con la antelación indicada, el cese de su actividad y el destino que se vaya a dar a los certificados, especificando en su caso si se va a transferir la gestión y a quien.
- Con carácter previo al cese definitivo de la actividad, comunicará al organismo de control, la información relativa a los certificados emitidos al público cuya vigencia haya sido extinguida para que se haga cargo de su custodia.
- Cualquier otra obligación que venga impuesta por la ley.

5.10. CARACTERÍSTICAS DE LOS CERTIFICADOS Y DE LA LISTA DE CERTIFICADOS

5.10.1. Características de los Certificados

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 servidor centralizado, 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 tienen 1 par de claves para “Firma Digital”,

Los certificados de usuario final a partir de su emisión, sea en token, archivo u otro contenedor que se incorpore; según se establezca podrán contener dos o únicamente un par de claves, de “Firma Digital”, mismo que se conformará con una clave pública y clave privada.

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 140-2 nivel 3 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 AC o AR de la ECIBCE o sus Tercero Vinculado. Pudiendo la ECIBCE o sus Terceros Vinculados prestar el servicio en línea siempre que el usuario mantenga en su poder un dispositivo reconocido.

En cuanto a los dispositivos móviles (IOS y Android), su propiedad, procedencia y titularidad es de exclusiva responsabilidad del solicitante de firma electrónica.

Los certificados de servidor seguro emitidos en modalidad offline, tienen 1 par de llaves, identificando en el mismo para el uso de clave "Firma Digital y "Cifrado".

Los certificados de sellado de tiempo, sirven para firmar electrónicamente estampas de tiempo de acuerdo a sus límites de uso. Este certificado, puede ser utilizado por quien brinde el servicio de estampado de tiempo.

Los certificados de OCSP, sirven para firmar las peticiones de validación en línea del estado de un certificado digital.

Más información de cada tipo de certificado consultar la Política de Certificados correspondiente, publicadas en el portal www.eci.bce.ec, sección "Marco Normativo".

5.10.2. Lista de Certificados

Los certificados una vez emitidos se publicarán en una base de datos o repositorio disponible públicamente. Esta operación será realizada por personal autorizado a partir de los archivos generados por la ECIBCE.

La lista de Certificados estará a disposición de los usuarios en la página web de la ECIBCE www.eci.bce.ec.

Los Certificados expirados y revocados aparecerán como tales en la CRL y serán archivados por la ECIBCE durante un periodo de quince (15) años.

5.10.3. Lista de Autoridades de Certificación Revocadas (ARL)

Una lista de autoridades de certificación revocadas, es simplemente un archivo que contiene los números de serie de los certificados de la AC Raíz y/o AC Subordinadas que hayan sido revocadas.

Las ARL's son firmadas cada nueve meses por la por la AC Raíz por procedimiento; o extraordinariamente, cuando se produzca la revocación de un certificado de autoridad subordinada.

5.10.4. Lista de Certificados Revocados (CRL)

La Entidad de Certificación de Información es responsable de indicar en los certificados que emita, la dirección en Internet de su página en donde se localizará la Lista de Certificados Revocados y el Protocolo de Estado de Certificados en Línea (OCSP), URL: <http://ocsp.eci.bce.ec>, para que de esta manera sea fácilmente accesible por los usuarios.

Las CRL's generadas por la ECIBCE tiene un tiempo de vigencia de 25 horas, la ECIBCE actualiza y publica la CRL cada vez que un certificado es revocado o antes del vencimiento de la vigencia de la CRL si no se presentan solicitudes de revocación.

Hay que recalcar que la ECIBCE mantiene en línea la verificación del estado de un certificado mediante un repositorio LDAP y/o el OCSP, es decir, una vez revocado un certificado, inmediatamente al firmar un documento o mensaje de datos, le mostrará un mensaje indicando que el certificado se encuentra revocado.

El Banco Central del Ecuador, a través de la Entidad de Certificación de Información, mantendrá actualizada las ARL's y CRL's, incluyendo todos los certificados revocados y expirados desde la última actualización.

A continuación, se muestra los campos que contiene una Lista de Certificados Revocados (CRL):

Formato de la CRL		
Campo	Descripción	Valor
Versión	Versión del Certificado estándar X509	V2
Emisor (issuer)	CN	AC BANCO CENTRAL DEL ECUADOR
	L	QUITO
	OU	ENTIDAD DE CERTIFICACIÓN DE INFORMACIÓN-ECIBCE
	O	BANCO CENTRAL DEL ECUADOR
	C	EC
Fecha Efectiva	Fecha de publicación	Fecha publicación de la CRL de la AC Subordinada
Fecha Próxima actualización	Fecha de vencimiento	Fecha de vencimiento de la CRL de la AC Subordinada
Algoritmo de firma	Algoritmo Hash que genera una síntesis de datos o huella digital	sha256RSA
Identificador de clave de entidad emisora	Id. de clave	18 f9 f0 fb e6 32 1c 99 66 39 2a ca 8b b2 69 7d 49 27 bf ce

5.11. CONTROLES DE SEGURIDAD FÍSICA, PROCEDIMENTAL Y DE PERSONAL

Este componente describe los controles físicos, procedimentales y de personal usados por la ECIBCE para realizar en forma segura las funciones de generación de llave, autenticación del

solicitante, emisión del certificado, revocación del certificado y archivado. Estos controles están descritos en el documento “Declaración de Políticas de Seguridad”.

5.12. FORMATOS

Las claves públicas de los certificados de la AC RAIZ y AC Subordinadas están disponibles en formatos .CER.

Las claves públicas de los certificados de usuario final están disponibles en el portal web de la ECIBCE www.eci.bce.ec.

La Lista de Certificados Revocados (CRL), se encuentra disponible en formato CRL V3, en el repositorio de la Entidad de Certificación de Información del Banco Central del Ecuador.

Los certificados en archivo tendrán un formato estándar PKCS#12, P12 o PFX, con protección mediante PIN o contraseña de la clave privada.

Los certificados para contenedor celular tendrán un formato estándar en PKCS#11, con protección mediante PIN o contraseña de la clave privada.

Los certificados para servidores seguros SSL serán entregados a los solicitantes en formato CER.

Las Políticas de Certificados de la Entidad de Certificación de Información del Banco Central del Ecuador, se encuentran en formato PDF.

Todas las versiones de la Declaración de Prácticas de Certificación son documentos públicos y se encuentran en formato PDF.

El certificado de la Entidad de Certificación de Información se encuentra disponible en el portal web de la entidad de certificación www.eci.bce.ec, en el Centro de descargas.

La revocación y suspensión de Certificados son instrumentos a utilizar en el supuesto de que por alguna causa establecida en la presente DPC se deje de confiar en el Certificado antes de la finalización de su período de validez originalmente previsto.

Los Usuarios de Certificados pueden consultar en cualquier momento el estado de un Certificado determinado, bien visitando la página web o bien realizando la solicitud correspondiente a través de un correo electrónico.

5.13. ACTUALIZACIÓN, PUBLICACIÓN Y NOTIFICACIÓN

5.13.1. Actualización de la Declaración de Prácticas de Certificación y de las Políticas de Certificados

La ECIBCE podrá actualizar la presente DPC y sus PCs, sin perjuicio de que se mantenga el nivel de calidad esencial de sus servicios de certificación y, siempre y cuando, toda actualización se justifique desde el punto de vista jurídico, técnico o comercial.

5.13.2. Publicación de las Actualizaciones

Las actualizaciones efectuadas sobre la DPC se darán a conocer a los interesados en la página web <http://www.eci.bce.ec> y en las oficinas de la AC y las AR.

5.13.3. Notificación de las Publicaciones

En caso que las actualizaciones efectuadas en la DPC incidan directamente en los derechos y obligaciones de los Suscriptores y/o Solicitantes, así como cuando dichas actualizaciones alteren la operatividad de los Certificados por parte de los usuarios, deberán notificarse dichas actualizaciones a los Suscriptores y/o Solicitantes con un período de antelación de quince (15) días término, a la aplicación de los cambios efectuados.

El transcurso de dicho periodo sin que medie comunicación escrita por parte del Suscriptor y/o Solicitante, en contra de las citadas actualizaciones implicará su aceptación. La no aceptación de las actualizaciones de esta DPC realizadas por la AC, tendrá como consecuencia la resolución de contrato con el suscriptor/solicitante y/o revocatoria solicitada por el usuario.

Se considerará como medio eficaz para la realización de notificaciones, el correo electrónico enviado a la dirección proporcionada por el Suscriptor y/o Solicitante.

ANEXO 2



BANCO CENTRAL DEL ECUADOR

**IG-052 POLÍTICAS DE CERTIFICADO -
PC CERTIFICADO DE FIRMA
ELECTRÓNICA DE PERSONA
NATURAL DE LA ENTIDAD DE
CERTIFICACIÓN DE INFORMACIÓN
DEL BANCO CENTRAL DEL ECUADOR
- ECIBCE**

OID: 1.3.6.1.4.1.37947.2.1.1

Marzo

2021

Este documento contiene la sexta versión de las Políticas de Certificado - OID: 1.3.6.1.4.1.37947.2.1.1 Certificado de Firma Electrónica de Persona Natural del Banco Central del Ecuador.

Versión 6.0

SUBGERENCIA DE SERVICIOS

DIRECCIÓN NACIONAL DE SERVICIOS FINANCIEROS

GESTIÓN DE CERTIFICACIÓN ELECTRÓNICA

© 2021. Dirección de Procesos, Calidad e Innovación- Coordinación General de Planificación y Gestión Estratégica - Banco Central del Ecuador.

Todos los derechos reservados.

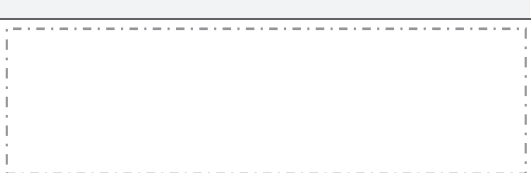
El presente documento no puede ser reproducido, distribuido, comunicado públicamente, archivado o introducido en un sistema de recuperación de información, o transmitido, en cualquier forma y por cualquier medio (electrónico, mecánico, fotográfico, grabación o cualquier otro), total o parcialmente, sin el previo consentimiento por escrito del Banco Central del Ecuador.

ÍNDICE

REVISIÓN Y APROBACIÓN.....	
CONTROL DE HISTORIAL DE CAMBIOS	
INFORMACIÓN GENERAL	
1. OBJETIVO	
2. BASE NORMATIVA.....	
3. GLOSARIO DE TÉRMINOS Y/O DEFINICIONES	
4. ÁMBITO DE APLICACIÓN	
5. CONTENIDO TÉCNICO DEL DOCUMENTO	
5.1. INTRODUCCIÓN E IDENTIFICACIÓN.....	
5.1.1. DETALLES DE CONTACTO	
5.2. COMUNIDAD DE USUARIOS Y APLICABILIDAD	
5.2.1. AUTORIDAD DE CERTIFICACION (AC).....	
5.2.2. AUTORIDAD DE REGISTRO (AR).....	
5.2.3. SOLICITANTE.....	
5.2.4. SUSCRIPTOR.....	
5.2.5. USUARIO	
5.3. NORMAS, ESTÁNDARES Y RFC REFERENCIADOS PARA LA ELABORACIÓN DE LA PC.....	
5.4. CERTIFICADO DE FIRMA ELECTRÓNICA DE PERSONA NATURAL.....	
5.4.1. ASPECTOS GENERALES	
5.4.1.1. Aplicación.....	
5.4.1.2. Datos incluidos en el certificado	
5.4.1.3. Usos del certificado y sus límites	
5.4.1.3.1. El certificado garantiza:	
5.4.1.4. Acceso a las claves y al certificado	
5.4.2. SOLICITUD DEL CERTIFICADO DE PERSONA NATURAL.....	
5.4.2.1. Requisitos del solicitante.....	
5.4.2.2. Identificación, emisión y entrega de certificados digitales (BCE o Tercero Vinculado_entrega presencial)	
5.4.2.3. Identificación, emisión y entrega de certificados digitales (atención en línea)	
5.4.2.4. Identificación, emisión y entrega de certificados digitales con nuevo portal web y conexión a plataformas de interoperabilidad gubernamental	

5.4.2.5. Plazos	
5.4.2.6. Emisión del certificado en diferentes contenedores.....	
5.4.2.7. Responsabilidades en la entrega	
5.4.3. REVOCACIÓN DEL CERTIFICADO DE FIRMA ELECTRÓNICA DE PERSONA NATURAL	
5.4.3.1. Supuestos de revocación	
5.4.3.2. Efectos de la Revocación	
5.4.3.3. Procedimiento de Revocación.....	
5.4.4. RENOVACIÓN DEL CERTIFICADO	
5.4.4.1. Requerimientos previos para la renovación de certificado de firma electrónica de persona natural	
5.4.4.2. Solicitud y procedimiento de renovación de un Certificado de Firma Electrónica de Persona Natural.....	
5.4.5. VALIDEZ DEL CERTIFICADO DE FIRMA ELECTRÓNICA DE PERSONA NATURAL	
5.4.6. ACEPTACIÓN DE CERTIFICADOS	
5.4.7. FIRMA Y ENTREGA DEL CONTRATO	

REVISIÓN Y APROBACIÓN

Elaborado por:	Firma
Especialista de Certificación Electrónica 1	 Firmado electrónicamente por: VICTOR MARCELO BALAREZO NOBOA
Especialista Administrativo 1	 Firmado electrónicamente por: DARWIN HUMBERTO PAZMINO LUCIO
Revisado y Validado por:	Firma
Subgerente de Servicios	 Firmado electrónicamente por: JOHN CARLOS ARROYO JACOME
Directora Nacional de Servicios Financieros	 Firmado electrónicamente por: MARITZA IVON VASCONEZ LOPEZ
Especialista de Medios de Pago 2	 Firmado electrónicamente por: NANCY ESTHELA CONDE CASTILLO
Aprobado por:	Firma
Gerente General	

CONTROL DE HISTORIAL DE CAMBIOS

Versión	Descripción del cambio	Fecha de actualización
1.0	Versión Inicial de las "IG-052 Políticas de Certificado - PC OID: 1.3.6.1.4.1.37947.2.1.1 Certificado de Firma Electrónica de Persona Natural	Junio - 2010
2.0	Actualización de las Políticas de Certificado - PC OID: 1.3.6.1.4.1.37947.2.1.1 Certificado de Firma Electrónica de Persona Natural	Marzo - 2011
3.0	Actualización de las Políticas de Certificado - PC OID: 1.3.6.1.4.1.37947.2.1.1 Certificado de Firma Electrónica de Persona Natural	Agosto - 2011
4.0	Actualización de las Políticas de Certificado - PC OID: 1.3.6.1.4.1.37947.2.1.1 Certificado de Firma Electrónica de Persona Natural, versión que incluye opción de certificado digital en contenedor celular; modifica el tiempo de vigencia de los certificados y actualiza las unidades administrativas involucradas, de acuerdo al Estatuto Orgánico de Gestión Organizacional por Procesos del Banco Central del Ecuador.	Julio - 2018
5.0	Versión actualizada del documento normativo "IG-052 Políticas de Certificado - PC OID: 1.3.6.1.4.1.37947.2.1.1 Certificado de Firma Electrónica de Persona Natural", se modifica el tiempo de archivo de solicitudes de certificados electrónicos de 2 meses a 1 mes y el tiempo de renovación de certificados caducados de 6 meses 2 meses después del vencimiento".	Agosto - 2019
6.0	Actualización de las Políticas de Certificado- PC OID 1.3.6.1.4.1.37947.2.1.1 Certificado de Firma Electrónica de Persona Natural; se elimina requisito: digitalizado de factura de servicios básicos correspondiente a la dirección domiciliaria del usuario; se incluye varios aspectos relativos a nuevos procesos de emisión en línea, procedimiento con nuevo portal web de la ECIBCE, se agrega el concepto de AC de Software Libre y actualización de cómputo de términos y plazos según lo establecido por el Código Orgánico Administrativo y comunicado mediante Circular Nro. BCE-CGJ-2020-0001-C de 08 de julio de 2020 y Memorando No. BCE-CGPGE-2020-0413-M de 03 de agosto de 2020.	Marzo - 2021

INFORMACIÓN GENERAL

TÍTULO	Políticas de Certificado - PC de la Entidad de Certificación de Información del Banco Central del Ecuador - ECIBCE OID: 1.3.6.1.4.1.37947.2.1. Certificado de Firma Electrónica de Persona Natural.
Autores:	Marcelo Balarezo Lorena Altamirano Dirección Nacional de Servicios Financieros
Vigencia:	El presente documento tendrá vigencia a partir de la fecha de su aprobación.
Aprobación:	Gerente General
Responsabilidad de la implementación, ejecución, del control previo y concurrente:	Subgerencia de Servicios. Dirección Nacional de Servicios Financieros. Gestión de Certificación Electrónica. Dirección Nacional de Riesgos de Operaciones. Dirección de Aseguramiento de la Calidad y Seguridad Informática. Gestión de Operación de Clave Pública.
Responsabilidad de la revisión y actualización:	El presente documento normativo será revisado y actualizado por las áreas previstas en <i>responsabilidad de la implementación, ejecución, del control previo y concurrente</i> .
Responsabilidad de la evaluación de control interno:	Dirección Nacional de Auditoría Interna Bancaria y/o Gubernamental, en el ámbito de su competencia.
Distribución:	El presente documento normativo será distribuido por la Dirección de Gestión Documental y Archivo a los servidores previstos en <i>responsabilidad de la implementación, ejecución, del control previo y concurrente</i> .

1. OBJETIVO

Establecer las políticas para la prestación de servicios de certificación de la Entidad de Certificación de Información del Banco Central del Ecuador (ECIBCE), aplicable a certificados de firma electrónica para Persona Natural.

2. BASE NORMATIVA

- Constitución de la República del Ecuador.
- Código Orgánico Administrativo.
- Ley Orgánica de Defensa del Consumidor.
- Ley Orgánica Transparencia y Acceso a la Información Pública.
- Ley Orgánica para la Optimización y Eficiencia de Trámites Administrativos y su Reglamento General.
- Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos y su Reglamento.
- Codificación de Resoluciones emitidas por la Junta de Política y Regulación Monetaria y Financiera, Libro I: Sistema Monetario y Financiero, Título I, Capítulo XV “Del Servicio de Entidad de Certificación de Información y Emisión de Certificados Digitales o Electrónicos”.
- Normas de Control Interno de la Contraloría General del Estado para las Entidades, Organismos del Sector Público y de las Personas Jurídicas de Derecho Privado que dispongan de Recursos Públicos.
- Acuerdo Ministerial No. 181 del 15 de septiembre de 2011, Acuerdo No. 006-2015 del 27 de enero de 2015 y Acuerdo No. 012-2016 emitidos por el Ministerio de Telecomunicaciones y de la Sociedad de la Información.
- Acuerdos Ministeriales o Resoluciones que expida el Ministerio de Telecomunicaciones y Sociedad de la Información MINTEL, sobre la materia
- Resolución ARCOTEL-2018-0902 del 25 de octubre de 2018, mediante la cual se renovó la acreditación del Banco Central del Ecuador como Entidad de Certificación de Información y Servicios Relacionados.
- Resoluciones y demás normativa conexa, expedida por la ARCOTEL.
- Estatuto Orgánico de Gestión Organizacional por procesos del Banco Central del Ecuador vigente.
- Resoluciones Administrativas del Banco Central del Ecuador.

- Normas Técnicas Ecuatorianas NTE INEN-ISO/IEC 27000 para la Gestión de la Seguridad de la Información, según actualice el Instituto Ecuatoriano de Normalización.
- Normas para Administración de Seguridad de Información del Banco Central del Ecuador (NT-001) de 27 de diciembre de 2017.

3. GLOSARIO DE TÉRMINOS Y/O DEFINICIONES

Con propósitos explicativos se mencionan los términos, definiciones y/o acrónimos utilizados a través del presente documento normativo.

- **AC:** Autoridad de Certificación.
- **Acuerdo de autoridad de registro:** contrato suscrito entre la ECIBCE y una entidad interna o externa al Banco Central del Ecuador, sea ésta pública o privada, que tiene como objeto regular la relación jurídica entre ambas partes para cumplir actividades de emisión, revocación y renovación de certificados digitales por delegación de la ECIBCE; así como brindar otros servicios relacionados.
- **AC Subordinada:** AC Banco Central del Ecuador, Autoridad de Certificación Subordinada del Banco Central del Ecuador, cuyo objetivo es emitir certificados a usuarios finales y firmar la lista de certificados revocados (CRL); así como certificados para autoridades de estampado de tiempo y OCSP (Online Certificate Status Protocol).
- **AC Subordinada de software libre:** Autoridad de Certificación Subordinada del Banco Central del Ecuador, que se basa en una tecnología PKI de software libre, es decir no propietario, por lo tanto, sin consumo de licencias de usuario final.
- **AC raíz BCE:** Autoridad de Certificación Raíz Banco Central del Ecuador, emite certificados a Autoridades de Certificación subordinadas y firma la lista de autoridades de certificación revocadas (**ARL**) y la lista de certificados revocados (**CRL**).
- **AR:** Autoridad de Registro.
- **ARCOTEL:** Agencia de Regulación y Control de las Telecomunicaciones.
- **ARL:** Lista de autoridades de certificación revocadas.
- **Autenticación:** es el proceso por el cual el certificado digital, que le pertenece al usuario, es validado por la Entidad Certificadora de Información del Banco Central del Ecuador.
- **Autoridad de certificación (AC – en inglés CA, Certification Authority-):** es la entidad de confianza, responsable de emitir y revocar certificados digitales de firma electrónica y que puede prestar otros servicios relacionados como la publicación de certificados, publicación de listas de certificados revocados (CRL), comprobación de validez de certificados, custodia electrónica, entre otros.

La prestación de servicios de certificación por parte de terceros será únicamente a través de la vinculación con una Entidad de Certificación Acreditada.

- **Autoridad de registro (AR):** dependencia/área del Banco Central del Ecuador o entidad pública/privada externa al Banco Central del Ecuador que en calidad de Tercero Vinculado a la ECIBCE, se encargará de recibir, validar, verificar y gestionar las solicitudes de emisión, revocación y renovación de certificados digitales de firma electrónica y otros servicios relacionados, cumpliendo con lo establecido en las políticas y procedimientos definidos en este documento y demás documentos normativos relacionados.
- **BCE:** Banco Central del Ecuador.
- **C:** Country (País). Atributo del Nombre Distintivo (DN) de un objeto dentro de la estructura de directorio X.500.
- **Certificado digital:** es un documento digital mediante el cual la autoridad de certificación asegura la vinculación entre la identidad del usuario, su clave pública y privada.
- **Certificado de firma electrónica:** el certificado de firma electrónica es un archivo (mensaje de datos), que certifica la vinculación de una firma electrónica con una persona determinada, a través de un proceso de comprobación que confirma su identidad.
 - **Certificados de firma electrónica de todo propósito:** son certificados de firma electrónica que sirven para firmar electrónicamente: correos electrónicos, facturas electrónicas, contratos electrónicos, ofertas del Sistema Nacional de Contratación Pública, transacciones electrónicas, trámites tributarios electrónicos, trámites de importaciones y exportaciones o cualquier otro tipo de aplicaciones donde se pueda reemplazar la firma manuscrita y se encuentre facultado para hacerlo dentro del ámbito de su actividad o límites de su uso. Se puede utilizar también para autenticación y cifrado de datos. Este certificado, puede ser utilizado por personas naturales o físicas, así como Personas Jurídicas.
 - **Certificado de persona natural o física:** son certificados que identifican al suscriptor como una persona natural o física y será responsable a título personal de todo lo que firme electrónicamente, dentro del ámbito de su actividad y límites de uso que correspondan.
- **Clave pública:** es la clave del certificado digital que se utiliza para la verificación de la firma electrónica y el cifrado de datos.
- **Clave privada:** es la clave confidencial que mantiene en privado el usuario. Usada generalmente para descifrar los mensajes codificados y también para generar la firma electrónica.

- **Claves RSA:** es el sistema criptográfico con clave pública. Es un algoritmo asimétrico que utiliza una clave pública, la cual se distribuye (en forma autenticada preferentemente), y otra privada, la cual es guardada en secreto por su propietario.
- **Cómputo de términos:** “Se excluyen del cómputo de términos los días sábados, domingos y los declarados feriados. Los días declarados como feriados en la jurisdicción de la persona interesada, se entenderán como tal, en la sede del órgano administrativo o viceversa”.
- **Cómputo de plazos:** “El plazo se lo computará de fecha a fecha. / Si en el mes de vencimiento no hay día equivalente a aquel en que comienza el cómputo, se entiende que el plazo expira el último día del mes”.
- **Common Criteria:** Criterios Comunes es un estándar con reconocimiento internacional para evaluar las funciones de seguridad y el nivel de confianza de un producto IT (ISO 15408).
- **CN:** Common Name (Nombre Común). Atributo del Nombre Distintivo (DN) de un objeto dentro de la estructura de directorio X.500.
- **Contenedor de certificado de firma electrónica:** el certificado de firma electrónica puede estar contenido en archivo digital (p12), roaming, dispositivo TOKEN, dispositivo criptográfico de seguridad HSM o en dispositivo móvil tipo Smartphone; éste último puede estar contenido mediante una aplicación (APP) que cumple con niveles de seguridad FIPS 140-1.
- **Contrato de prestación de servicios de certificación:** documento jurídico que tiene por objeto regular los derechos y obligaciones derivados de la prestación de los servicios de certificación por la ECIBCE, al suscriptor.
- **CRL:** Certificate Revocation List (Lista de Certificados Revocados).
- **CSR:** Certificate Signing Request (Petición de firma del certificado), estándar PKCS#10.
- **Datos:** datos únicos que se registran de acuerdo a lo siguiente:
 - **Datos de creación de firma:** son datos únicos, como códigos o claves criptográficas privadas, que el suscriptor utiliza para crear la firma electrónica.
 - **Datos de verificación de firma:** son los datos, como códigos o claves criptográficas públicas, que se utilizan para verificar la firma electrónica, mediante el uso de herramientas o aplicaciones destinadas para esta finalidad.
- **DINARDAP:** Dirección Nacional de Registro de Datos Públicos.
- **DIGERCIC:** Dirección General de Registro Civil, Identificación y Cedulación.
- **Dispositivo criptográfico portable seguro - TOKEN:** elemento físico donde se almacena en forma segura el certificado de firma electrónica que será emitido por la ECIBCE.

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).

- **Distinguished Name (DN):** nombre Distintivo, son los campos que sirve para identificar a un certificado digital, que además es único.
- **DN:** Distinguished Name (Nombre Distintivo). Identificación unívoca de una entrada dentro de la estructura de directorio X.500.
- **Documento de identidad válido:** cédula de ciudadanía, de identidad, pasaporte y demás documentos que la legislación ecuatoriana admita como válidos para acreditar la identidad de una persona.
- **DPC - Declaración de Prácticas de Certificación:** documento que reúne las reglas que la ECIBCE utiliza para gestión, administración, homologación, generación, uso y conservación de cada uno de los certificados de firma electrónica, así como de los servicios relacionados que ofrece.
- **En línea:** El concepto se utiliza en el ámbito de la informática para referirse a algo o a alguien que está haciendo uso de la red Internet.
- **ECI:** Entidad de Certificación de Información.
- **ECIBCE - Entidad de certificación de información y servicios relacionados del Banco Central del Ecuador:** es el Banco Central del Ecuador que emite certificados de firma electrónica y que puede prestar otros servicios relacionados con la firma electrónica, autorizada por el Consejo Nacional de Telecomunicaciones, ahora Agencia de Regulación y Control de Telecomunicaciones, según lo dispuesto en Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos y su Reglamento General.

Las autoridades de registro de la ECIBCE, serán las encargadas de la verificación de documentos e identificación de los solicitantes y suscriptores del certificado de firma electrónica, mediante el procedimiento definido vigente; para luego completar el proceso de emisión de certificados.

- **ETSI:** European Telecommunications Standard Institute.
- **FIPS - Federal Information Processing Standard:** son estándares de seguridad del Gobierno Estadounidense para el procesamiento de la información”; para el caso de la ECIBCE y ésta DPC, son niveles de seguridad requeridos para el dispositivo TOKEN que puede comprender todo el dispositivo criptográfico; a nivel externo, de 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. Los FIPS son avalados por el NIST (National Institute of Standards and Technology).

- **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.
- **HSM -Módulo de seguridad criptográfico (Hardware Security Module):** empleado para almacenar claves y realizar operaciones criptográficas de modo seguro, aporta aceleración de hardware para operaciones criptográficas. Módulo de seguridad criptográfico empleado para almacenar claves y realizar operaciones criptográficas de modo seguro.
- **Identificación:** reconocimiento fehaciente de la identidad del suscriptor del signatario de un certificado.
- **ISO:** International Organization for Standardization.
- **ITU-T o UIT:** Unión Internacional de Telecomunicaciones que es el organismo especializado en telecomunicaciones de la Organización de las Naciones Unidas, encargado de regular las telecomunicaciones a nivel internacional entre las distintas administraciones y empresas operadoras.
- **L:** Localidad. Atributo del Nombre Distintivo (DN) de un objeto dentro de la estructura de directorio X.500.
- **LDAP:** Lightweight Directory Access Protocol (Protocolo de acceso a servicios de directorio).
- **Lista de certificados revocados (CRL):** es una lista de certificados que han sido revocados, que no son válidos y en los que no debe confiar ningún usuario del sistema.
- **MINTEL:** Ministerio de Telecomunicaciones y de la Sociedad de la Información.
- **NITS:** National Institute of Standards and Technology, por sus siglas en inglés, Instituto Nacional de Normas y Tecnología - es una agencia de la Administración de Tecnología del Departamento de Comercio de los Estados Unidos (cuya misión es promover la innovación y la competitividad industrial EE.UU. haciendo avanzar la ciencia de medición, normas, y la tecnología de forma que mejoren la seguridad económica y calidad de vida).
- **Notario Público:** servidor público encargado de emitir documentos de acuerdo con las solemnidades requeridas por la legislación ecuatoriana.
- **O:** Organization. Atributo del Nombre Distintivo (DN) de un objeto dentro de la estructura de directorio X.500.
- **OCSP - Online Certificate Status Protocol:** Este protocolo permite comprobar en línea la vigencia de un certificado electrónico, método para determinar el estado de revocación de un certificado digital X.509 en línea.

- **OID:** object identifier (Identificador de objeto único), son una representación numérica universal y única que permite la identificación de objetos por una metodología que asegura unicidad; cumple con Normas Internacionales. La estructura OID para los certificados de información contiene campos comunes para las Autoridades de Certificación, esta norma es utilizada para definir las políticas de certificados de información y para los certificados digitales.
- **ORGANISMO DE CONTROL:** ARCOTEL
- **OU:** Organizational Unit. Atributo del Nombre Distintivo (DN) de un objeto dentro de la estructura de directorio X.500.
- **PC:** Políticas de Certificados.
- **Persona natural o física:** todos los individuos de la especie humana,
- **PFX O P12:** Es un archivo de seguridad con clave privada de un certificado digital.
- **PIN:** Personal Identification Number (Número de Identificación Personal o contraseña).
- **PKCS:** Public Key Cryptography Standards. Estándares de PKI desarrollados por RSA Laboratories y aceptados internacionalmente.
- **PKI - Public Key Infrastructure (Infraestructura de Clave Pública):** en criptografía, una infraestructura de clave pública es una combinación de hardware y software, políticas y procedimientos de seguridad que permiten la ejecución con garantías de operaciones criptográficas como el cifrado, la firma digital o el no repudio de transacciones electrónicas. El software que incluye la PKI puede ser de software propietario (licenciado) o de software libre.
- **PKIX:** Grupo de trabajo del IETF (Public Key Infrastructure X509 IETF Working Group) constituido con el objeto de desarrollar las especificaciones relacionadas con las PKI e Internet.
- **Política de Certificado (PC o CP, "Certification Policy" en inglés):** contiene las reglas a las que se sujeta el uso de los certificados definidos en la política. Se describen los papeles, responsabilidades y relaciones entre el usuario final y la Autoridad de Certificación y las reglas de solicitud, adquisición gestión y uso de los certificados. Este documento matiza y complementa a la Declaración de Prácticas de Certificación (DPC) de la Autoridad de Certificación.
- **Prestador de servicios de certificación:** empresa o persona jurídica que expide certificados o presta otros servicios en relación con la firma electrónica.
- **Registro:** proceso directo e indelegable por el cual el Solicitante o el Suscriptor consigna en una solicitud, toda la información relacionada con él.
- **RFC:** Request For Comments (Estándar emitido por la IETF).

- **Revocación/ revocatoria:** efecto de la pérdida de fiabilidad del certificado digital de firma electrónica, originando el cese permanente de la operatividad, conforme a los usos que le son propios.
- **SSL - Secure Sockets Layer (Protocolo para comunicación segura):** es un protocolo criptográfico que proporciona comunicación segura por una red, comúnmente Internet.
- **Servicio en línea:** Nuevos servicios que prestará la ECIBCE de forma directa o a través de Terceros Vinculados, mediante el uso de tecnologías de la información para el reconocimiento o identificación de las personas con validación biométrica facial y con el acceso a un botón de pagos.
- **Servidor:** es una computadora que, formando parte de una red, provee servicios a otras computadoras denominadas clientes.
- **SN:** Surname (apellido). Atributo del Nombre Distintivo (DN) de un objeto dentro de la estructura de directorio X.500.
- **Solicitante:** la persona natural o jurídica que solicita la emisión de un Certificado por parte de la ECIBCE, sometiéndose al procedimiento de verificación de identidad y de creación del certificado de firma electrónica que la ECIBCE ha establecido para su emisión.
- **Suscriptor:** es la persona natural a favor de la cual se ha emitido un certificado. Los suscriptores deberán ajustarse a lo señalado en la DPC, en la PC del certificado que han obtenido y, en su caso, en el contrato de Prestación de Servicios suscrito con la ECIBCE. Los suscriptores deberán ajustarse a los procedimientos establecidos para la petición de cada tipo de certificado, y cumplir los requisitos que se establezcan en esta DPC.
- **Tercero vinculado:** con sujeción al artículo 33 de la Ley de Comercio Electrónico, firmas y mensajes de datos, la Prestación de Servicios de Certificación de información podrá ser proporcionada por parte de terceros, para lo cual deberá demostrar su vinculación con la Entidad de Certificación de Información y Servicios Relacionados Acreditada ante el CONATEL, ahora Agencia de Regulación y Control de las Telecomunicaciones ARCOTEL.
- **TSA:** Time Stamping Authority (Autoridad de Sellado de Tiempo).
- **TST:** Time Stamp TOKEN (Sello Digital de Tiempo).
- **Umbral límite (K,N) de SHAMIR:** esquemas criptográficos visuales secretos.
- **Usuario:** la persona natural o persona Jurídica que confía en un Certificado emitido por la ECIBCE.
- **UTF8:** Unicode Transformation Format - 8 bits.

- **X.500:** es un conjunto de estándares de redes de ordenadores de la ITU-T sobre servicios de directorio.
- **X.509:** especifica formatos estándar para certificados de claves públicas y un algoritmo de validación de la ruta de certificación.

4. ÁMBITO DE APLICACIÓN

- BCE Matriz Quito.
- BCE Dirección Zonal Guayaquil.
- BCE Dirección Zonal Cuenca.
- Terceros Vinculados.
- Solicitantes y Usuarios de Firma Electrónica.

5. CONTENIDO TÉCNICO DEL DOCUMENTO

5.1. INTRODUCCIÓN E IDENTIFICACIÓN

El presente documento describe la Política de Certificación (PC) de la Entidad de Certificación de Información del Banco Central del Ecuador - ECIBCE para los Certificados de Firma Electrónica de Persona Natural.

Esta política pormenoriza y completa lo establecido en la Declaración de Prácticas de Certificación (DPC) de la ECIBCE, recogiendo un conjunto de reglas que indican los procedimientos seguidos por la ECIBCE en la prestación de sus servicios (solicitud, identificación, aceptación, emisión y revocación) así como los límites de uso, el ámbito de aplicación y las características técnicas de este tipo de certificado.

La Política de Certificación puede ser consultada por Internet, en la página web de la ECIBCE <https://www.eci.bce.ec/marco-normativo> o en la página web del Banco Central del Ecuador <https://www.bce.fin.ec/index.php/servicios-bancarios>, en la sección Productos y Servicios seleccionar Certificación Electrónica, o personalmente en las oficinas de la ECIBCE.

La Política de Certificación, está dirigida a cualquier persona que confíe de buena fe, legalidad y legitimidad en este tipo de certificados.

Todos los solicitantes y suscriptores de certificados antes de recibir el certificado deben conocer este documento.

5.1.1. DETALLES DE CONTACTO

Nombre	Entidad de Certificación de Información del Banco Central del Ecuador
Correo electrónico	eci@bce.ec
Dirección	Av.10 de Agosto N11-409 y Briceño
Número de teléfono	(593) 2 3938600 Ext. 2863, 2831, 2873, 2841, 2031
Sitio Web	https://www.eci.bce.ec

5.2. COMUNIDAD DE USUARIOS Y APLICABILIDAD**5.2.1. AUTORIDAD DE CERTIFICACION (AC)**

EL Banco Central del Ecuador es la Autoridad Certificadora (AC) o Entidad de Certificación de Información (ECI), que relaciona una determinada clave pública con una persona natural, a través de la emisión de un certificado digital de firma electrónica, de conformidad con los términos de esta PC y con la DPC de la ECIBCE.

5.2.2. AUTORIDAD DE REGISTRO (AR)

La ECIBCE podrá asignar el proceso de registro y comprobación de identidades, en una o varias Autoridades de Registro (AR) o Terceros Vinculados. Estas Autoridades de Registro deberán comprobar la identidad inequívoca de los solicitantes de acuerdo con las normas de esta PC, de la DPC y del Acuerdo o Contrato para Autoridad de Registro.

La ECIBCE podrá también gestionar por medio de contratos de AR o de Terceros Vinculados, con entidades externas al Banco Central del Ecuador ya sean estas de carácter público o privado, las mismas que ejecutarán los procedimientos normados para las AR vinculadas al Banco Central del Ecuador.

5.2.3. SOLICITANTE

A los efectos de esta PC, se entenderá por solicitante a la persona natural, que solicita la emisión de un certificado por parte de la ECIBCE, sometiéndose al procedimiento de verificación de identidad y de creación del certificado de firma electrónica que la ECIBCE ha establecido para su emisión.

5.2.4. SUSCRIPTOR

El suscriptor es la persona natural a favor de quien se ha emitido un certificado.

Los suscriptores deberán ajustarse a lo señalado en la DPC, en la PC del certificado que han obtenido y, en su caso, en el contrato de prestación de servicios suscrito con la ECIBCE.

Los suscriptores deberán ajustarse a los procedimientos establecidos para la petición de cada tipo de certificado, y cumplir los requisitos que se establezcan en esta PC.

5.2.5. USUARIO

Se entiende por usuario del certificado a la persona que voluntariamente confía y hace uso de los Certificados de la ECIBCE emitido en diferentes contenedores de certificados de firma electrónica (token, archivo, roaming, HSM, dispositivo móvil tipo smartphone).

Cuando el usuario decida voluntariamente confiar y hacer uso del certificado le será aplicable esta PC, así como la DPC.

5.3. NORMAS, ESTÁNDARES Y RFC REFERENCIADOS PARA LA ELABORACIÓN DE LA PC

- RFC 3739 "Internet X.509 Public Key Infrastructure Qualified Certificates Profile".
- RFC 3280 "Internet X.509 Public Key Infrastructure Certificate and CRL Profile".
- RFC 3647: "Internet X.509 Public Key Infrastructure. Certificate Policy and Certification Practices Framework".
- ETSI TS 101 862 "Qualified certificate profile".
- ISO/IEC 9595 - "Distinguished Name (DN)".
- Norma ISO/IEC 9594-8 estándar x.509.

5.4. CERTIFICADO DE FIRMA ELECTRÓNICA DE PERSONA NATURAL

Sirve para el propósito que se le otorgue, dentro de las limitaciones legales y técnicas, permite identificar a una persona natural quien será responsable a título personal de todo lo que firme, en forma electrónica, dentro del ámbito de su actividad y límites de su uso que correspondan.

Toda la información contenida en el certificado es suministrada a la entidad que actúa como Autoridad de Registro por el propio suscriptor bajo su entera responsabilidad, y resulta como información del suscriptor verificada, de acuerdo con lo establecido en la PC de la ECIBCE.

La comprobación de la identidad del solicitante/suscriptor será presencial, documental y/o en línea a través de la validación de sistemas biométricos, y mediante el uso del servicio de

consumo de datos de la DINARDAP o ficha de datos del Registro Civil u otras que se pongan a disposición.

El solicitante/suscriptor deberá presentarse ante la Autoridad de Registro o Tercero Vinculado, portando su documento de identificación (cédula o pasaporte válido), suficientemente claro y actualizado para permitir su inequívoca identificación.

El solicitante/suscriptor podrá conectarse en línea ante la Autoridad de Registro o Tercero Vinculado, pasando por un proceso de validación de identidad, a través de un sistema biométrico, que permitirá su inequívoca identificación; o de ser el caso, podrá realizar la validación de identidad mediante sesión de videoconferencia.

Todos los datos contenidos en el certificado se protocolizan de acuerdo con lo establecido en la DPC y en la PC del certificado de firma electrónica de persona natural.

- Este certificado se emite en las siguientes modalidades:
- Dispositivos criptográficos seguros formato PKCS#11 (TOKEN).
- Dispositivos criptográficos seguros con estándar PKCS#10 (HSM).
- Dispositivos móviles (teléfono inteligente o tableta) con estándar PKCS#11.
- Almacenamiento en archivo estándar PKCS#12 (PFX O P12).
- Almacenamiento en Servidor Roaming.

5.4.1. ASPECTOS GENERALES

5.4.1.1. Aplicación

En este tipo de certificados se relaciona la identidad de un suscriptor con su clave pública, y permite la firma de documentos, mensajes de datos y transacciones electrónicas, para lo cual se aplicará la legislación ecuatoriana vigente referida a la firma electrónica.

5.4.1.2. Datos incluidos en el certificado

Los datos que se incluirán en un Certificado de Firma Electrónica de persona natural emitido por la ECIBCE serán los siguientes:

Formato del certificado digital de persona natural		
Campo	Descripción	Valor
Versión	Versión del Certificado estándar X509	V3
Número de serie	Número que identifica unívocamente al certificado	Número de serie del certificado
Algoritmo de firma	Algoritmo utilizado por la ECIBCE para firmar el certificado	sha256RSA

Formato del certificado digital de persona natural		
Campo	Descripción	Valor
Algoritmo hash de firma	Algoritmo de encriptación utilizado por la ECIBCE para firmar el certificado	sha256
Emisor	CN	AC BANCO CENTRAL DEL ECUADOR
	L	QUITO
	OU	ENTIDAD DE CERTIFICACIÓN DE INFORMACIÓN-ECIBCE
	O	BANCO CENTRAL DEL ECUADOR
	C	EC
Válido desde	Fecha y hora UTC desde que es válido el certificado	Fecha de inicio de la validez del certificado de persona natural
Válido hasta	Fecha y hora UTC hasta la cual es válido el certificado	Fecha final de la validez del certificado de persona natural
Sujeto	CN	NOMBRES Y APELLIDOS
	Número de Serie	Número de Serie secuencial
	L	QUITO
	OU	ENTIDAD DE CERTIFICACIÓN DE INFORMACIÓN-ECIBCE
	O	BANCO CENTRAL DEL ECUADOR
	C	EC
Clave pública	Clave pública del suscriptor	RSA (2048 bits)
Uso de la clave	Descripción del uso de la clave	Firma digital (80) o Cifrado de clave (20)
Directivas o Bases del Certificado	Identificador de Objetos según la normalización internacional de la IANA	1.3.6.1.4.1.37947.2.1.1 http://www.eci.bce.ec/politica-certificado/persona-natural.pdf
Acceso a la información de la entidad emisora	Método para la validación en línea del estado del certificado	Direcciones URL del método de acceso OCSP
Nombre alternativo	Nombre alternativo X509v3	Nombre RFC822= correo electrónico del suscriptor
Puntos de distribución CRL	Punto de distribución de lista de certificados revocados	Direcciones URL del punto de distribución
Identificador de clave de entidad emisora	Código hash entidad emisora	Hash entidad emisora

Formato del certificado digital de persona natural		
Campo	Descripción	Valor
Identificador de clave del titular	Código hash del certificado del usuario	Hash del certificado
Restricciones básicas	Restricciones de tipo de usuario y de longitud de ruta	Tipo de usuario = Entidad final Restricción de longitud de ruta = Ninguno
1.2.840.113533.7.65.0	Identificador de versión de plataforma PKI	V8.1
Algoritmo de identificación	Algoritmo Hash que genera una síntesis de datos o huella digital para las firmas digitales	SHA1
Huella digital	La síntesis o huella digital de los datos del certificado	Id de huella asociado al certificado
1.3.6.1.4.1.37947.3.1	OID atributo cédula o pasaporte	CÉDULA O PASAPORTE (Obligatorio)
1.3.6.1.4.1.37947.3.2	OID atributo Nombres	NOMBRES COMPLETOS (Obligatorio)
1.3.6.1.4.1.37947.3.3	OID atributo Apellido 1	APELLIDO 1 (Obligatorio)
1.3.6.1.4.1.37947.3.4	OID atributo Apellido 2	APELLIDO 2 (Obligatorio)
1.3.6.1.4.1.37947.3.7	OID atributo dirección	DIRECCIÓN (Obligatorio)
1.3.6.1.4.1.37947.3.8	OID atributo teléfono	TELÉFONO (Obligatorio)
1.3.6.1.4.1.37947.3.9	OID atributo ciudad	CIUDAD (Obligatorio)
1.3.6.1.4.1.37947.3.12	OID atributo País	PAÍS (Opcional)
1.3.6.1.4.1.37947.3.11	OID atributo RUC	RUC (Opcional)
1.3.6.1.4.1.37947.3.50	OID atributo RUP	RUP (Opcional)
1.3.6.1.4.1.37947.3.51	OID atributo contenedor	CONTENEDOR (Opcional)

5.4.1.3. Usos del certificado y sus límites

Este tipo de certificado se utilizará para:

- Firmar documentos electrónicos.
- Firmar mensajes de correo electrónico que soporten protocolo S/MIME.
- Autenticar servidor.

- Identificar y autenticar el acceso autorizado de una persona natural a un sistema o aplicativo.

Por las características esenciales del certificado, éste podría ser utilizado para otras finalidades y en concreto, para el cifrado y descifrado de documentos o mensajes electrónicos. No obstante, este uso es de exclusiva responsabilidad del suscriptor y/o del usuario del certificado. En todos los casos, la ECIBCE se deslinda de toda responsabilidad en el uso del certificado de persona natural por parte del suscriptor.

5.4.1.3.1. El certificado garantiza:

- **Identificación del suscriptor**

El suscriptor del certificado puede autenticar, frente a otra parte, su identidad, demostrando la asociación de su clave pública, contenida en el certificado, con el uso de su clave privada.

- **Integridad del documento firmado**

La utilización de este certificado garantiza que el documento firmado es íntegro, es decir, garantiza que el documento no fue alterado o modificado después de firmado por el suscriptor. Se certifica que el mensaje recibido es el mismo que fue emitido por el suscriptor.

- **No repudio de origen**

Con el uso de este certificado también se garantiza que la persona que firma el documento (suscriptor) no puede repudiarlo, es decir, el suscriptor que ha firmado no puede negar la autoría o la integridad del documento o correo firmado.

- **Confidencialidad**

Permite el acceso solo a las personas autorizadas y ofrece seguridad recíproca entre las partes.

La ECIBCE no asume ningún tipo de responsabilidad, ya sea legal, contractual o extra contractual, derivada de daños directos o indirectos por la utilización del certificado para tal finalidad, debido a que, por motivos de seguridad, esta Política determina que la ECIBCE no guarde copia de la clave privada del suscriptor.

Los certificados sólo podrán ser empleados con los límites y para los usos para los que hayan sido emitidos en cada caso.

El uso de los certificados que implique la realización de operaciones no autorizadas según las Políticas de Certificados aplicables a cada uno de los certificados, la DPC y los contratos de la ECIBCE con sus suscriptores tendrá la consideración de usos indebidos, a los efectos legales oportunos, eximiéndose por tanto la ECIBCE, en función de la legislación vigente, de cualquier responsabilidad por este uso indebido de los certificados que realice el suscriptor o cualquier tercero.

En función de los servicios prestados por la ECIBCE mediante la emisión de sus certificados, no es posible por parte de la ECIBCE el acceso o conocimiento del contenido del mensaje al que haya sido adjuntado o con el que se relacione el uso de un certificado emitido por la ECIBCE. Por lo tanto, y como consecuencia de esta imposibilidad técnica de acceder al contenido del mensaje, no es posible por parte de la ECIBCE emitir valoración alguna sobre dicho contenido, asumiendo por tanto el suscriptor cualquier responsabilidad procedente del contenido de dicho mensaje unido al uso de un certificado emitido por la ECIBCE.

Asimismo, le será imputable al suscriptor cualquier responsabilidad que pudiese derivarse de la utilización del mismo fuera de los límites y condiciones de uso recogidas en las Políticas de Certificados aplicables a cada uno de los certificados, la DPC y los contratos de la ECIBCE con sus suscriptores, así como de cualquier otro uso indebido del mismo derivado de este apartado o que pueda ser interpretado como tal en función de la legislación ecuatoriana vigente sobre firma electrónica.

Las políticas definidas garantizan que los nombres distintivos (DN) de los certificados son suficientemente significativos para vincular la clave pública con la identidad del usuario.

Las reglas utilizadas para la interpretación de los nombres distintivos en los certificados emitidos están descritas en la ISO/IEC 9595 (DN). Adicionalmente todos los certificados emitidos utilizan codificación UTF8 para todos los atributos, según la RFC 3280 UNICIDAD DE LOS NOMBRES.

La Entidad de Certificación de Información del Banco Central del Ecuador, define como campo DN (Distinguished Name) del Certificado de Autoridad como único y sin ambigüedad. Para ello se incluirá como parte del DN, específicamente en el campo OU, el nombre o razón social de la Entidad de Certificación de Información del Banco Central del Ecuador. Por lo tanto, la unicidad se garantiza mediante la confianza sobre la unicidad del nombre.

La Entidad de Certificación de Información del Banco Central del Ecuador, no actúa como árbitro, mediador o conciliador, ni resuelve ninguna disputa relativa a la titularidad de nombres de personas u organizaciones, nombres de dominio, marcas o nombres comerciales, entre otros. Asimismo, esta Institución se reserva el derecho de rechazar una solicitud de certificado debido a conflictos de nombres de usuarios finales.

5.4.1.4. Acceso a las claves y al certificado

- **Contenedor de certificados en dispositivos criptográficos seguros, tipo TOKEN**

El soporte para el almacenamiento de las claves y el certificado será un dispositivo criptográfico.

El acceso al dispositivo criptográfico, donde se encuentra la clave privada, se realizará a través de contraseña (PIN). Para realizar una firma electrónica es necesario introducir el PIN que únicamente conoce el suscriptor. En la generación de las claves no se permite realizar una copia de seguridad de las mismas.

- **Contenedor de certificados en dispositivos criptográficos seguros, tipo HSM (Hardware Security Module)**

El contenedor para el almacenamiento de las claves y el certificado será el dispositivo criptográfico seguro, tipo HSM, el mismo que deberá cumplir con los niveles de seguridad internacionales.

La ECIBCE no se responsabiliza por las copias generadas por el suscriptor, es responsabilidad de éste el uso del certificado y su almacenamiento seguro. Deberá considerar las políticas de seguridad para el acceso al mismo. Si se daña o se borra el certificado y sus claves será necesario realizar una revocación previo a un nuevo proceso de emisión.

- **Contenedor de certificados en archivo formato PKCS#12 (PFX o P12)**

El contenedor para el almacenamiento de las claves y el certificado será un archivo. El suscriptor deberá disponer de las medidas de seguridad que garanticen inequívocamente que el uso del certificado está limitado exclusivamente al suscriptor del certificado. El acceso para la instalación del certificado se realizará a través de un PIN o contraseña.

La ECIBCE no se responsabiliza por las copias generadas por el suscriptor, es responsabilidad del suscriptor del uso del certificado y custodia, deberá considerar políticas de seguridad para el acceso al mismo. Si se daña o se borra el certificado y sus claves, será necesario realizar una revocación, previo a un nuevo proceso de emisión del certificado.

- **Contenedor de certificados en dispositivos móviles PKCS#11**

Las claves públicas y privadas de los certificados podrán ser emitidas a personas naturales y custodiadas en un dispositivo móvil (celular inteligente o tablet), dicho contenedor está definido para almacenar las llaves privadas con estándares de seguridad al momento de acceder a la información de manera segura y cifrada.

Los usuarios de este servicio deberán acceder por medio de un PIN a la aplicación que efectuará el proceso de firma electrónica, confirmando la acción mediante una notificación al dispositivo móvil, para la autenticación y uso del certificado digital.

- **Contenedor de certificados en Servidor Roaming**

Las claves públicas y privadas de los certificados podrán ser emitidas a personas naturales y custodiadas en un servidor centralizado de la ECIBCE del Banco Central del Ecuador, dicho servidor está definido para brindar el servicio de Roaming, con estándares de seguridad al momento de acceder a la información.

Los usuarios de este servicio deberán acceder por medio de un PIN o CONTRASEÑA para la autenticación y uso del certificado digital a través de un software proporcionado por la ECIBCE o a través de un API.

El atributo que identificará que el certificado digital está almacenado en un contenedor ya sea HARDWARE o SOFTWARE está definido por el siguiente identificador de objeto:

OID: 1.3.6.1.4.1.37947.3.51

5.4.2. SOLICITUD DEL CERTIFICADO DE PERSONA NATURAL

5.4.2.1. Requisitos del solicitante

Para ser solicitante y de ser el caso, posteriormente suscriptor de este tipo de certificados, el solicitante o el suscriptor debe contar con la siguiente documentación, sea presentada de forma directa u obtenida a través de interconexión de datos públicos que se disponga:

- Digitalizado a color de la cédula (o ficha de datos de cédula) o pasaporte vigente con visa de residencia temporal o permanente o diplomático.
- 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 (CNE) en este ámbito. O confirmación que se encuentra habilitado para trámite público por el CNE.
- Señalar en la solicitud, la dirección exacta y actualizada del domicilio del solicitante o suscriptor del certificado de firma electrónica, bajo declaración de veracidad de la información proporcionada.

En caso de simplificación, automatización o trámites en línea:

- Cuando el usuario acceda a servicios en línea, simplificados o automatizados de certificación electrónica de forma previa, deberá aceptar que conoce y acepta que la ECIBCE o su Tercero Vinculado, podrá obtener la cédula de identidad del solicitante o su equivalente (base de datos, ficha de datos u otro), así como la confirmación que se encuentra habilitado para trámite público por CNE (cumplimiento de votación), a través de sistemas o plataformas de interoperabilidad gubernamental, como el bus de datos de DINARDAP; cuando éstos no hayan sido presentados directamente por el solicitante a través del portal web, o en su defecto para cumplir con procesos de simplificación de trámites. No obstante, de no contar con la información obtenida a través de la plataforma indicada, la ECIBCE o sus Terceros Vinculados podrán requerir la presentación de los documentos digitalizados.

En caso de existir un cambio de documento de identificación:

- Al adquirir un certificado digital de firma electrónica Persona Natural con el tipo de identificación “pasaporte”, y en caso que ésta haya obtenido la cédula de identidad ecuatoriana no aplica la renovación; sin embargo, podrá pedir la revocatoria del certificado y solicitar un nuevo certificado con la cédula o podrá esperar a su

vencimiento para obtener el nuevo certificado (lo mismo aplica en caso de cambio de número de pasaporte).

5.4.2.2. Identificación, emisión y entrega de certificados digitales (BCE o Tercero Vinculado_entrega presencial)

- a) 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, y sube a la web en formato electrónico toda la información requerida o en su defecto, el sistema obtiene la información o documentación del usuario a través de plataformas de interoperabilidad gubernamental (cuando se habilite). Así también, la ECIBCE podrá habilitar a través de su portal web el proceso de emisión mediante el acceso de usuario, clave del solicitante o suscriptor e imagen de seguridad.
- b) 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 le requerirá al usuario corregir las inconsistencias encontradas y deberá ingresar una nueva solicitud. En caso que “Si fuera correcta”, se aprobará la solicitud y notificará al correo del solicitante/suscriptor registrado que debe realizar el pago.
- c) Una vez realizado el pago por cualquiera de los medios señalados en la página web de la ECIBCE y registrado en la AR, el sistema de certificación automáticamente remitirá un correo electrónico al solicitante/suscriptor para proceder con la identificación y emisión del certificado solicitado.
- d) El solicitante/suscriptor deberá presentarse con el documento de identificación, sea éste cédula o pasaporte válido, suficientemente claro y actualizado para permitir su inequívoca identificación, ante la Autoridad de Registro de la ECIBCE o el Tercero Vinculado.
- e) Identificado el suscriptor, la AR confrontará el documento de identificación (digital y original aportado), y en caso de conformidad procederá a la emisión del certificado y respectivamente a la firma del contrato de prestación del servicio y de la solicitud registrada.
- f) Para la emisión en HSM se requerirá adicionalmente la presencia de un delegado técnico del suscriptor.

5.4.2.3. Identificación, emisión y entrega de certificados digitales (atención en línea)

Nota:

Válido únicamente a partir de su implementación, según se informe a través del portal web www.eci.bce.ec.

Para acceder al servicio en línea, requerirá un computador, tablet o celular tipo smartphone, con acceso a una cámara web.

- a) Las solicitudes en línea para emisión, renovación o revocación de certificados digitales de firma electrónica aplicarán únicamente para contenedores Archivo, Roaming y contenedor Celular o dispositivo móvil tipo smartphone. El servicio será prestado directamente por la ECIBCE o Tercero(s) Vinculado(s) a la Entidad.
- b) El solicitante accede al portal WEB de www.eci.bce.ec, ingresa a la opción del servicio en línea; y, registra la información requerida a la persona natural como tipo de contenedor, de ser el caso selecciona el Tercero Vinculado, número de cédula, código dactilar u otro dato de la cédula, fotografía de cédula (si el sistema lo requiere para validaciones); acepta las condiciones del servicio para validaciones biométricas y/o capturas de fotografías de rostro del solicitante, etc.; agrega información que sea necesaria como datos de información personal y de actividad económica, direcciones físicas y correo(s) electrónico(s), entre otros datos, que permiten la identificación fehaciente del solicitante.
- c) Bajo el esquema de servicio en línea, el sistema obtendrá la información o documentación del usuario (cédula y papeleta de votación) a través de plataformas de interoperabilidad gubernamental, como el bus de datos de la DINARDAP o de Registro Civil, junto a este proceso se utilizará mecanismos o sistemas de validación o identificación biométrica facial con cruce de información; y, en el caso de no pasar en forma exitosa la validación biométrica, el usuario deberá ingresar su solicitud en el portal web para la emisión con atención presencial.

Según determine la ECIBCE, se permitirá la conexión mediante sesión de videoconferencia, como una opción adicional para validaciones e identificación del usuario solicitante, que se requiere realizar para la implementación del servicio de atención en línea.

- d) El sistema aprobará la solicitud en línea.
- e) El usuario realizará el pago en línea, a través, del botón de pagos puesto a disposición de la ciudadanía, por parte del Tercero Vinculado.
- f) Aprobada la solicitud y recibido el pago en línea, el usuario seguirá las instrucciones para la generación del certificado digital.

- g) Generado el certificado, el usuario ingresa una contraseña de seguridad correspondiente al Certificado digital en el tipo de contenedor seleccionado por el usuario (excepto token).
- h) El usuario suscribe el Contrato y Solicitud generados, con el certificado de firma electrónica que se emitió y se descarga su certificado digital, así como para su respaldo los documentos firmados electrónicamente.
- i) El usuario recibe la notificación del proceso concluido.
- j) En caso de errores del sistema, falta de validación, etc., el usuario deberá informar a la ECIBCE o al Tercero Vinculado o servicio de chat en línea.

5.4.2.4. Identificación, emisión y entrega de certificados digitales con nuevo portal web y conexión a plataformas de interoperabilidad gubernamental

Nota: Válido únicamente a partir de su implementación según se informe a través de www.eci.bce.ec

- a) El solicitante accede al nuevo portal web de certificación electrónica, debe “Ingresar al Sistema” de Certificación (en el menú), selecciona “Registro de Usuario Nuevo” (si es la primera vez) o Iniciar Sesión (cuando ya tiene usuario creado):

“Registro de Usuario Nuevo”:

- Selecciona tipo de identificación, ingresa número de identificación y captcha de seguridad; ingresa nombres completos si no se obtuvieron de la plataforma de interoperabilidad, correo electrónico, selecciona “Registrar”, el usuario recibirá en su correo electrónico el link de activación de la cuenta de acceso al sistema;
- Ingresa al link de Activación de Usuario del Sistema de Certificación Electrónica, verifica datos ingresados, registra un nombre de usuario (de 8 a 16 caracteres alfanuméricos, no usar Ñ, ñ y caracteres especiales), correo electrónico alternativo, selecciona imagen como factor de autenticación, acepta check de condiciones de uso y da clic en “Activar cuenta”.
- Recibe en su correo electrónico, una notificación de cuenta activada con el nombre de usuario que eligió y una clave temporal para acceder al portal y que debe cambiar como primer paso.

Iniciar Sesión para completar Registro de Usuario Nuevo:

- Ingresa usuario y clic en “Ingresar”, selecciona imagen de seguridad, marca “Siguiendo”, ingresa contraseña temporal enviada al correo electrónico, cerrar teclado virtual y da clic en Iniciar Sesión.

- Completar la información personal solicitada y cambiar la contraseña temporal por una definitiva (mínimo 8 caracteres, máximo 16, alfanumérico, una minúscula, una mayúscula y un carácter especial @\$%) y clic en “Guardar y Continuar”, la respuesta será que usuario se registró correctamente.
 - Y ya puede acceder con normalidad al sistema
- b) “Iniciar Sesión”, ingresa el usuario, selecciona imagen y clave de acceso; ingresa a la opción requerida “Solicitar certificado Digital” según los pasos que se desplegarán:
- a. Registro: tipo de certificado (p. natural), tipo de contenedor y uso del certificado,
- b. Datos Personales: nombres y apellidos, direcciones, números telefónicos, correo electrónico, RUC y RUP personal, información laboral,
- c. Requisitos: Cédula o pasaporte, papeleta de votación y pago de servicios se deberán subir en archivo pdf (de ser el caso los datos de la cédula y papeleta de votación se podrán obtener directamente del enlace a bus de datos de la DINARDAP). Además, el sistema le permitirá registrar cualquier excepción legal de no contar con papeleta de votación.
- d. Pre-factura: Le permitirá al usuario seleccionar y conocer el costo a cancelar, correspondiente al certificado digital y si desea adquirir el contenedor token y el valor total,
- e. Lugar de Entrega: Entidad, ciudad y oficina donde se acercará a retirar el certificado y,
- e. Finalización: Se despliega un resumen de la solicitud ingresada como nombres y apellidos, tipo de certificado, tipo de contenedor y lugar de entrega. Acepta la información contenida es verídica y marca “enviar” solicitud, con la respuesta de “Registro guardado correctamente”.
- c) El responsable del registro o quien cuente con el perfil respectivo en la ECIBCE o su Tercero Vinculado; accede al Sistema de Certificación, ingresa a cada una de las solicitudes en estado “Registrado”, verifica y/o valida la información consignada, en base a esto aprueba, rechaza o archiva la solicitud y se remite un correo automático de notificación al solicitante.
- d) En caso de contar con la solicitud aprobada, el usuario se puede acercar a realizar el pago correspondiente, y a la emisión de su certificado,
- e) El solicitante/suscriptor deberá presentarse con el documento de identificación, sea éste cédula o pasaporte válido, suficientemente claro y actualizado para permitir su inequívoca identificación, ante la Autoridad de Registro de la ECIBCE o el Tercero Vinculado.
- f) Identificado el suscriptor, la AR confrontará el documento de identificación (digital y original aportado), y en caso de conformidad procederá a la emisión y entrega del certificado y requerirá la firma del contrato de prestación del servicio y de la solicitud registrada.

5.4.2.5. Plazos

- Si el solicitante no realiza el pago en un plazo de un (1) mes, desde la fecha de aprobación de su solicitud, se archivará la solicitud.
- Si el solicitante no acude a la emisión del certificado en un plazo máximo un (1) mes contado a partir del correo enviado para la emisión del certificado se archivará la solicitud y el solicitante/suscriptor deberá ingresar una nueva solicitud.
- Si el suscriptor detecta la existencia de algún error en la información almacenada en su certificado de firma electrónica, previa notificación y de manera presencial o remota (si es el caso), se procederá con la revocación y la emisión de un nuevo certificado con los datos correctos; para lo cual tiene ocho (8) días término, excepto en el caso de requerir que se agregue el número de RUC en el certificado de persona natural, podrá extenderse hasta un plazo máximo un (1) mes; para comunicar a la ECIBCE a través del BCE, Tercero Vinculado y/o Autoridad de Registro.

5.4.2.6. Emisión del certificado en diferentes contenedores

- **En dispositivos criptográficos seguros, tipo TOKEN**
 - ✓ El responsable de emisión de la AR ECIBCE o Tercero Vinculado conecta el dispositivo criptográfico asignado al solicitante, en el módulo de emisión y validación de certificados.
 - ✓ El módulo de validación y emisión de certificados ejecuta las siguientes operaciones:
 - Genera automáticamente la clave privada en el dispositivo criptográfico.
 - Envía el CSR 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)**
 - ✓ 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 a la AC donde se firmará en modo offline.
 - El certificado es devuelto por la AC e instalado en el HSM.
- **En Archivo**
 - ✓ El responsable de emisión de la AR ECIBCE o Tercero Vinculado 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 a la AC donde se firmará en modo en línea (online).
 - El certificado es devuelto por la AC al equipo asignado.

✓ **Emisión en línea a través del Entorno Seguro de la ECIBCE:**

El responsable de emisión de la AR ECIBCE o Tercero Vinculado 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 un link exclusivo para el ingreso al Entorno Seguro del BCE, que se envía al correo electrónico registrado por el solicitante.
- Genera automáticamente el certificado de firma electrónica en el Entorno Seguro.
- El usuario registra su clave de uso del certificado y de forma unísona suscribe la Solicitud y el Contrato.

• **En Roaming**

- ✓ El responsable de emisión de la AR ECIBCE o Tercero Vinculado 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 a la AC donde se firmará en modo en línea (online).
 - El certificado es devuelto por la AC al servidor (equipo) asignado.

• **En dispositivos móvil (teléfono inteligente)**

- ✓ El responsable de emisión de la AR ECIBCE o Tercero Vinculado, 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 dispositivo móvil.
 - Envía el CSR a la AC donde se firmará en modo en línea (online).
 - El certificado es devuelto por la AC e instalado en el dispositivo.

5.4.2.7. Responsabilidades en la entrega

- El suscriptor debe comprobar en la propia AR ECIBCE o Tercero Vinculado que los datos del certificado son correctos y que corresponden a los suyos.
- La AR ECIBCE o Tercero Vinculado 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 almacenará el contrato y la solicitud en el gestor documental y remitirá al suscriptor vía correo electrónico los archivos firmados electrónicamente.

✓ **Emisión en línea:**

- El suscriptor debe comprobar que los datos del certificado son correctos y que corresponden a los suyos.
- La AR (Tercero Vinculado) 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.
- El suscriptor deberá descargar del Entorno Seguro habilitado, su certificado digital de firma electrónica en contenedor archivo y guardar.
- El suscriptor podrá descargar su Contrato y su Solicitud firmados.
- La AR / Tercero Vinculado y la ECIBCE almacenará el contrato y la solicitud firmados.
- La ECIBCE remitirá al suscriptor vía correo electrónico los documentos firmados electrónicamente por el suscriptor.
- La AR/Tercero Vinculado y la ECIBCE NO guarda ni almacena el certificado digital generado en el Entorno Seguro.

5.4.3. REVOCACIÓN DEL CERTIFICADO DE FIRMA ELECTRÓNICA DE PERSONA NATURAL

5.4.3.1. Supuestos de revocación

Los Certificados de persona natural deberán ser revocados cuando concurra alguna de las circunstancias siguientes:

- Solicitud voluntaria del Suscriptor.
- Olvido de clave (aplica una recuperación del certificado sin costo y con costo a partir del segundo olvido).
- Uso no permitido del certificado.

- Pérdida o inutilización por daños del soporte del certificado o modificación del certificado.
- Utilización indebida del certificado por el suscriptor o por terceros.
- Fallecimiento del suscriptor.
- Inexactitudes en los datos aportados por el solicitante para la obtención del certificado, así como la concurrencia de circunstancias que provoquen que dichos datos, originalmente incluidos en el certificado, no se adecúen a la realidad.
- Por error en la emisión del certificado debido a una no adecuación al procedimiento establecido en la PC prevista para el Certificado de Persona Natural y/o, en su caso, en el contrato establecido entre la ECIBCE y el suscriptor.
- Que se detecte que las claves privadas del Suscriptor han sido comprometidas, bien porque concurren las causas de pérdida, robo, hurto, modificación, divulgación o revelación de las claves privadas, bien por cualquier otra circunstancia, incluidas las fortuitas, que indiquen el uso de las claves privadas por persona distinta al titular.
- Por incumplimiento por parte de la AR, la ECIBCE o el Suscriptor de las obligaciones establecidas en la DPC.
- Por cualquier causa que razonablemente induzca a creer que el servicio de certificación haya sido comprometido hasta el punto que se ponga en duda la fiabilidad del certificado.
- Por resolución judicial o administrativa que lo ordene.
- Por la concurrencia de cualquier otra causa especificada en la Ley, la Declaración Prácticas de Certificación y la presente Política de Certificación.
- Por las causas que se establecen en los literales a) y b) del artículo 26 y literal b) del artículo 37 de la Ley de Comercio Electrónico, Firmas Electrónicas y Mensaje de Datos:

"Art. 26.- Revocatoria del certificado de firma electrónica.- El certificado de firma electrónica podrá ser revocado por el Consejo Nacional de Telecomunicaciones, de conformidad con lo previsto en esta Ley, cuando:

- a) La entidad de certificación de información cese en sus actividades y los certificados vigentes no sean asumidos por otra entidad de certificación; y,*
- b) Se produzca la quiebra técnica de la entidad de certificación judicialmente declarada."*

"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:

- 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; (...)*

En cualquier caso, en todas las solicitudes de revocación se deberá comprobar fehacientemente la identidad del solicitante de la revocación.

5.4.3.2. Efectos de la Revocación

- El efecto de la revocación del certificado de firma electrónica de persona natural es la pérdida de fiabilidad del mismo, originando el cese permanente de la operatividad del certificado conforme a los usos que le son propios y, en consecuencia, de la prestación de los servicios de certificación.
- La revocación de un certificado impide el uso legítimo del mismo por parte del suscriptor.
- La revocación del certificado por causa no imputable al suscriptor originará la emisión de un nuevo certificado a favor del suscriptor por el plazo restante para concluir el período originario de validez del certificado revocado o de ser el caso por un nuevo plazo a partir de la nueva emisión.
- La revocación del certificado tendrá como consecuencia la notificación a terceros de que un certificado ha sido revocado, cuando se solicite la verificación del mismo.

5.4.3.3. Procedimiento de Revocación

Solicitarán la revocación, llenando la solicitud correspondiente en el portal de Certificación Electrónica de la ECIBCE y/o a través del servicio en línea de Terceros Vinculados.

Así también, la ECIBCE, a través de su portal web o de ser el caso del servicio en línea proporcionado directamente o por sus Terceros Vinculados; podrá habilitar el proceso de autogestión de revocatorias de certificados, mediante el acceso de usuario y clave del suscriptor y/o ingreso del número de serie del certificado y código OTP recibido en el correo electrónico registrado por el suscriptor.

En cuanto tengan conocimiento de la concurrencia de alguna de las circunstancias contempladas en el apartado 5.4.3.1:

- El solicitante/suscriptor del certificado de persona natural.
- La AR, respecto a aquellos certificados en cuya emisión hayan participado.

Asimismo, podrá solicitar la revocación cualquier tercero con un interés legítimo en caso de que tenga conocimiento de la existencia alguna de las siguientes causas:

- Pérdida del soporte del certificado.

- Fallecimiento del suscriptor.
- Inexactitudes en los datos de información del certificado.
- Compromiso de la fiabilidad del certificado.
- Compromiso de las claves.

En todo caso la ECIBCE o su Tercero Vinculado podrá de oficio, iniciar el procedimiento de revocación de certificados, en cualquiera de los casos previstos en el apartado 5.4.3.1.

La autoridad judicial o administrativa podrá, en aquellos supuestos que señale la Ley, así como las demás disposiciones vigentes, instar a la ECIBCE a revocar el certificado. La solicitud de revocación de certificados se podrá dirigir a la ECIBCE o ante la AR, en su caso, por medio de oficio o bien acercándose personalmente ante la AR, en su caso.

Aquel que solicite la revocación deberá identificarse con cualquier medio válido en derecho y justificar la solicitud aportando la documentación que acredite la existencia del hecho que origina la petición de la revocación.

Cuando la persona que solicite la revocación del Certificado de Firma Electrónica de persona natural no sea el propio suscriptor, deberá dirigirse y gestionar de forma presencial y mediante oficio motivado en cualquiera de las oficinas de la ECIBCE o las AR, en su caso.

Una vez recibida y verificada la solicitud de revocación, la ECIBCE procederá a tramitar la revocación efectiva del certificado. La decisión de revocar un certificado corresponde a la ECIBCE.

La decisión de revocar el certificado será comunicada por la ECIBCE al suscriptor mediante correo electrónico a la dirección consignada en la petición del certificado.

Igualmente, se publicará la revocación del certificado en la CRL. La publicación de la CRL de la ECIBCE se realiza cada 10 minutos o cada vez que se revoca un certificado, la vigencia de la CRL es de 25 horas.

La consulta se puede realizar vía web en:

http://www.eci.bce.ec/CRL/eci_bce_ec_crlfilecomb.crl

<http://ocsp.eci.bce.ec/ejbca/publicweb/status/ocsp>

<ldap://bceqldapsubp1.bce.ec/>

La revocación comenzará a producir efectos frente a terceros a partir de su publicación por parte de la ECIBCE, salvo que la causa de revocación sea el cese de la actividad de prestación de servicios de certificación de la ECIBCE, en cuyo caso, la pérdida de eficacia tendrá lugar desde que esa circunstancia se produzca.

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, ésta deberá realizar los esfuerzos que razonablemente estén a su alcance para restablecer el servicio en el menor tiempo posible.

5.4.4. RENOVACIÓN DEL CERTIFICADO

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

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.

Para la renovación de su certificado de firma electrónica, el usuario podrá modificar sus datos que considere necesarios a excepción de sus nombres, número o documento de identidad y el tipo de contenedor del certificado de firma electrónica.

En la renovación deberá ingresar a la página web y remitir la documentación actualizada, conforme se señala en el numeral 5.4.2.1.

Los certificados emitidos por la ECIBCE tienen un plazo de vigencia establecido en el propio certificado y siempre será acorde con la legislación vigente. Se podrá acudir a los trámites para la renovación de los servicios de certificación si concurren las circunstancias recogidas en esta PC.

Los requerimientos previos, la forma de solicitar la renovación y el procedimiento de renovación de certificados serán los que se especifican en las PC de cada certificado.

5.4.4.1. Requerimientos previos para la renovación de certificado de firma electrónica de persona natural

Deberán concurrir los siguientes:

- Que el suscriptor desee la renovación del servicio de certificación, y lo comunique con una antelación máxima de dos (2) meses, antes de que concluya la vigencia de su certificado y hasta dos (2) meses posteriores.
- Que lo solicite en debido tiempo y forma, siguiendo las instrucciones y normas que la ECIBCE especifica para tal efecto.
- Que la ECIBCE no haya tenido conocimiento cierto de la concurrencia de ninguna causa de revocación/suspensión del certificado.
- Que la totalidad de los datos incluidos en el certificado sean los mismos que en el momento de la emisión del certificado.
- Que la solicitud de renovación del certificado se refiera al mismo tipo de certificado emitido inicialmente.

- Que se haya satisfecho el pago correspondiente por la renovación del certificado. Observar el plazo establecido en el numeral 5.4.2.5.

5.4.4.2. Solicitud y procedimiento de renovación de un Certificado de Firma Electrónica de Persona Natural

- a) El suscriptor que solicite la renovación del certificado de Firma Electrónica deberá completar el formulario que encontrará a su disposición en la página web del portal de la ECIBCE.
- b) El suscriptor, además del envío de la solicitud deberá pagar el valor correspondiente a la renovación a través de cualquiera de los medios indicados en la página web de la ECIBCE o del Tercero Vinculado. Si el suscriptor no solicitara según lo establece la DPC y las PC, en debida forma la renovación y dentro del plazo determinado, deberá solicitar la emisión de un nuevo certificado, con el pago de valores que correspondan a la emisión y no tendrá derecho a reclamo alguno.
- c) El solicitante accede al portal WEB de la ECIBCE o a través del servicio en línea de Terceros Vinculados, registra toda la información en el formulario de solicitud de renovación de certificado de persona natural, y sube a la web en formato electrónico todos los requisitos habilitantes, de ser el caso se podrá obtener documentos como cédula de identidad o su equivalente y papeleta de votación o equivalente a través de la interconexión a la plataforma de interoperabilidad gubernamental. Así también, la ECIBCE podrá habilitar el acceso al portal web mediante el ingreso de usuario, clave e imagen de seguridad para ingreso de la solicitud de renovación de un certificado digital de firma electrónica.
- d) El responsable del registro o quien cuente con el perfil respectivo, en la ECIBCE o su Tercero Vinculado; una vez que el solicitante accede al portal WEB de la ECIBCE, registra toda la información en el formulario de solicitud de renovación de certificado de persona natural y sube a la web en formato electrónico todos los requisitos habilitantes; verificará meticulosamente la información consignada. En caso de que ésta “no sea correcta”, se le requerirá al usuario subsanar las inconsistencias encontradas y deberá ingresar una nueva solicitud. En caso que “Si fuera correcta”, se aprobará la solicitud y notificará automáticamente al correo del solicitante/suscriptor registrado, para que realice el pago correspondiente.
- e) Una vez realizado el pago por cualquiera de los medios señalados en la página web de la ECIBCE y registrado en la AR en el sistema de certificación electrónica, se acercará o acudirá a la emisión del certificado digital.

En el caso de servicios en línea con Terceros Vinculados, el pago se realizará mediante el uso del botón de pago habilitado para el efecto o transferencias bancarias.

- f) El suscriptor se deberá presentar con el documento de identificación, sea éste cédula o pasaporte válido, suficientemente claro y actualizado para permitir su inequívoca identificación, ante la Autoridad de Registro de la ECIBCE o el Tercero Vinculado.

Y en el caso de servicio en línea a través de Terceros Vinculados, la identificación será mediante un mecanismo de validación biométrica facial exitosa y presentación digital de su cédula de identidad a fin de permitir su identificación de forma inequívoca.

- g) Identificado el suscriptor, la AR confrontará el documento de identificación (digital y original aportado), y en caso de conformidad procederá a la emisión del certificado y respectivamente a la firma del contrato de prestación del servicio y de la solicitud registrada.

En el caso de servicios en línea a través de Terceros Vinculados, el usuario recibirá un link a su correo electrónico, que le permitirá acceder al Entorno Seguro de la ECIBCE, en el cual luego de aceptar el “Acuerdo de Términos y Condiciones”, generará su certificado digital de firma electrónica renovado, suscribiendo de forma unísona el Contrato y la Solicitud junto con el Tercero Vinculado.

5.4.5. VALIDEZ DEL CERTIFICADO DE FIRMA ELECTRÓNICA DE PERSONA NATURAL

- El período de validez o vigencia máxima del Certificado de Firma Electrónica de Persona Natural es de dos (2) años en cualquier tipo de contenedor (Token, HSM, Archivo o Roaming o dispositivo móvil tipo teléfono inteligente), desde su emisión, pasado el cual 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.

5.4.6. 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.

No obstante, a partir de la entrega del certificado, el suscriptor dispondrá de ocho (8) días término para revisar el mismo, determinar si es adecuado y si los datos corresponden con la realidad.

En caso de que existiera alguna diferencia entre los datos suministrados a la ECIBCE y el contenido del certificado, 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.

5.4.7. 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 ECIBCE y Tercero Vinculado archivará una copia.

La AR realizará la entrega física o en línea según corresponda del certificado digital al usuario, de acuerdo al tipo de contenedor solicitado en el que está el certificado; excepcionalmente se podrá entregar únicamente de forma física a una tercera persona, siempre y cuando presente un poder debidamente notariado.

La Autoridad de Registro/Tercero Vinculado y la ECIBCE NO guarda ni almacena el certificado digital generado en el Entorno Seguro.

RESOLUCIÓN No. SB-DTL-2021-0474

LUIS ANTONIO LUCERO ROMERO
DIRECTOR DE TRÁMITES LEGALES

CONSIDERANDO:

QUE el artículo 228 del Código Orgánico Monetario y Financiero establece que las entidades del sistema financiero nacional tendrán un auditor externo registrado y calificado en cuanto a su idoneidad y experiencia por la superintendencia correspondiente;

QUE el artículo 4, del capítulo I “Normas para la contratación y funcionamiento de las auditoras externas que ejercen su actividad en las entidades sujetas al control de la Superintendencia de Bancos”, del título XVII “Calificaciones otorgadas por la Superintendencia de Bancos”, del libro I “Normas de control para las entidades de los sectores financieros público y privado” de la Codificación de las Normas de la Superintendencia de Bancos, establece los requisitos para la calificación de los auditores externos, personas naturales;

QUE el Ingeniero en Finanzas, Diego Ramiro Vallejo Arteaga, mediante comunicación ingresada al Sistema de Calificaciones con hoja de ruta No. SB-SG-2021-02615-E, ingresó la documentación para la calificación como auditor externo, la misma que reúne los requisitos exigidos en las normas vigentes;

QUE el último inciso del artículo 6 del citado capítulo I, establece que la calificación otorgada por la Superintendencia de Bancos tendrá una vigencia de diez (10) años, contados desde la fecha de emisión de la resolución de calificación;

QUE mediante memorando N° SB-DTL-2021-0567-M de 26 de febrero de 2021, se establece que el Ingeniero en Finanzas, Diego Ramiro Vallejo Arteaga, cumple con los requisitos determinados en el citado capítulo I; y,

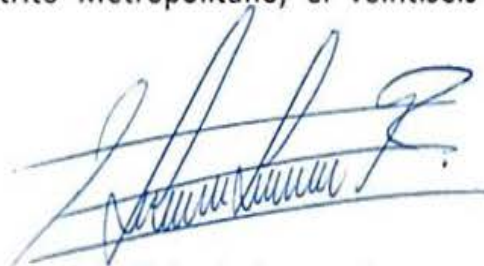
EN ejercicio de las atribuciones delegadas por el Superintendente de Bancos mediante resolución No. SB-2019-280, de 12 de marzo de 2019; y, resolución No. ADM-2021-14787, de 17 de febrero de 2021,

RESUELVE:

ARTÍCULO 1.- CALIFICAR al Ingeniero en Finanzas, Diego Ramiro Vallejo Arteaga portador de la cédula de ciudadanía No. 1713438917, para que pueda desempeñar las funciones de auditor externo en las entidades sujetas al control de la Superintendencia de Bancos; la presente resolución de calificación tendrá una vigencia de diez (10) años, contados desde la fecha de emisión de la misma.

ARTÍCULO 2.- DISPONER que se incluya la presente resolución en el registro de auditores externos, se le asigne el registro No. AEQ-2021-00085; y, se comunique del particular a la Superintendencia de Compañías, Valores y Seguros.

COMUNÍQUESE Y PUBLÍQUESE EN EL REGISTRO OFICIAL.- Dada en la Superintendencia de Bancos, en Quito, Distrito Metropolitano, el veintiséis de febrero del dos mil veintiuno.



Mgs. Luis Antonio Lucero Romero
DIRECTOR DE TRÁMITES LEGALES

LO CERTIFICO.- En Quito, Distrito Metropolitano, el veintiséis de febrero del dos mil veintiuno.



Dra. Silvia Jeaneth Castro Medina
SECRETARIA GENERAL





Ing. Hugo Del Pozo Barrezueta
DIRECTOR

Quito:
Calle Mañosca 201 y Av. 10 de Agosto
Telf.: 3941-800
Exts.: 3131 - 3134

www.registroficial.gob.ec

El Pleno de la Corte Constitucional mediante Resolución Administrativa No. 010-AD-CC-2019, resolvió la gratuidad de la publicación virtual del Registro Oficial y sus productos, así como la eliminación de su publicación en sustrato papel, como un derecho de acceso gratuito de la información a la ciudadanía ecuatoriana.

“Al servicio del país desde el 1º de julio de 1895”

El Registro Oficial no se responsabiliza por los errores ortográficos, gramaticales, de fondo y/o de forma que contengan los documentos publicados, dichos documentos remitidos por las diferentes instituciones para su publicación, son transcritos fielmente a sus originales, los mismos que se encuentran archivados y son nuestro respaldo.