RESOLUCIÓN ADMINISTRATIVA NO. BCE-GG-104-2019
ANEXO 1

BANCO CENTRAL DEL ECUADOR

POLÍTICAS DE CERTIFICADO - PC DE LA ENTIDAD DE CERTIFICACIÓN DE INFORMACIÓN DEL BANCO CENTRAL DEL ECUADOR – ECIBCE

OID: 1.3.6.1.4.1.37947.2.1.1

CERTIFICADO DE FIRMA ELECTRÓNICA DE PERSONA NATURAL

Agosto

2019

Este documento contiene la quinta 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 5.0

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

ÍNDICE

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

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.
Responsabilidad de la implementación y 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 *Responsabilidad de la Ejecución, del Control Previo y Concurrente.*
Responsabilidad de la evaluación de control interno:	Dirección Nacional de Auditoría Interna Bancaria y/o Gubernamental, en el ámbito de su competencia.

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

- Artículo 226 de la Constitución de la República del Ecuador.
- Ley Orgánica de Defensa del Consumidor.
- Ley Orgánica Transparencia y Acceso a la Información Pública.
- Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos y su Reglamento General.
- Codificación de Resoluciones Monetarias, Financieras, de Valores y Seguros, 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 para las Entidades, Organismos del Sector Público y de las Personas Jurídicas de Derecho Privado que dispongan de Recursos Públicos.
- Normas Técnicas Ecuatorianas NTE INEN-ISO/IEC 27000 para la Gestión de la Seguridad de la Información.
- Acuerdo Ministerial No. 181 de 15 de septiembre de 2011 del Ministerio de Telecomunicaciones y de la Sociedad de la Información.
- Acuerdo No. 012-2016 de 24 de junio de 2016 del Ministerio de Telecomunicaciones y de la Sociedad de la Información.
- Resolución ARCOTEL-2018-0902 Registro de la Acreditación como Entidad de Certificación de Información y Servicios Relacionados.
- Normativa legal relacionada expedida por el ARCOTEL.
- Normativa legal emitida por el MINTEL.
- Estatuto Orgánico de Gestión Organizacional por procesos del Banco Central del Ecuador.
- Resoluciones Administrativas emitidas por el Banco Central del Ecuador que aplique a certificación electrónica.
- Normas para la Administración de la Seguridad de la Información del Banco Central del Ecuador.

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 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, 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 sirvenpara 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.
- **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).
- **Datos:** datos único 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.
- **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.
- **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 Organizational for Standarization.
- **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.
- **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.

- **PKIX:** Grupo de trabajo del IETF (Public Key Infrastructure X509 IEFT Working Group) constituido con el objeto de desarrollar las especificación 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.
- **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. 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 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

6. COMUNIDAD DE USUARIOS Y APLICABILIDAD

6.1 AUTORIDAD DE CERTIFICACION (AC)

La ECIBCE actúa como Autoridad Certificadora (AC) relacionando una determinada clave pública con una persona natural o sitio Web concretos a través de la emisión de un certificado de conformidad con los términos de esta PC y con la DPC de la ECIBCE.

6.2 AUTORIDAD DE REGISTRO (AR)

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

La ECIBCE podrá también gestionar por medio de contratos de AR, 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.

6.3 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.

6.4 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 DPC.

6.5 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 teléfono inteligente).

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

7. 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.

8. CERTIFICADO DE FIRMA ELECTRÓNICA DE PERSONA NATURAL

Sirve para todo propósito 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 mediante el uso del servicio web con la DINARDAP.

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

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 formato PKCS#10 (HSM).
- Dispositivos móvil (teléfono inteligente) formato PKCS#11.
- Almacenamiento en archivo formato PKCS#12 (PFX O P12).
- Almacenamiento en Servidor Roaming.

8.1 ASPECTOS GENERALES

8.1.1 Aplicación

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

8.1.2 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
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

Formato del certificado digital de persona natural		
Campo	**Descripción**	**Valor**
	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
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)

Formato del certificado digital de persona natural		
Campo	Descripción	Valor
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)

8.1.3 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.

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.

8.1.3.1 El certificado garantiza:

- **Identificación del suscriptor**

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

- **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.

  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 firmante.

  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.

8.1.4 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 debe conocer 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

8.2 SOLICITUD DEL CERTIFICADO DE PERSONA NATURAL

8.2.1 Requisitos del solicitante

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

- Digitalizado a color de la 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 en este ámbito).

- Digitalizado de la factura de luz, agua o teléfono de los últimos tres meses que certifique la dirección domiciliaria.

En caso de existir un cambio de documento de identificación:

- Al adquirir un certificado digital de firma electrónica con el tipo de identificación "pasaporte", y en caso de obtener la cédula de identidad ecuatoriana no aplica la renovación; podrá pedir la revocatoria del certificado y solicitar un nuevo certificado con la cédula o deberá esperar a su vencimiento para obtener el nuevo certificado.

8.2.2 Identificación, emisión y entrega

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.

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 subsanar 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.

8.2.3 Plazos

- Si el solicitante no realiza el pago en un plazo de 30 días calendario 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 de 30 días calendario contados 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, tiene de 2 días laborables para comunicar a la ECIBCE a través del BCE, Tercero Vinculado y/o Autoridad de Registro. En este caso previa notificación y de manera presencial se procederá con la revocación y la emisión de un nuevo certificado con los datos correctos.

8.2.4 Emisión del certificado en diferentes contenedores

- **En dispositivos criptográficos seguros, tipo TOKEN**

  ✓ El responsable de emisión de la AR 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 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.

- **En Roaming**

  ✓ El responsable de emisión de la AR establece el mecanismo de emisión y validación del certificado, que será asignado al solicitante.

  ✓ El módulo de validación y emisión de certificados ejecuta las siguientes operaciones:

  - Genera automáticamente la clave privada en el servidor Roaming destinado para la emisión.
  - Desde el servidor asignado se envía el CSR 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 mecanismo para proceder con la emisión y entrega del certificado en este tipo de contenedor, se lo publicará una vez que el servicio esté disponible.

8.2.5 Responsabilidades en la entrega

- El suscriptor debe comprobar en la propia AR que los datos del certificado son correctos y que corresponden a los suyos.

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

- La AR almacenará el contrato y la solicitud en el gestor documental y remitirá al suscriptor vía correo electrónico los archivos firmados electrónicamente.

8.3 REVOCACIÓN DEL CERTIFICADO DE FIRMA ELECTRÓNICA DE PERSONA NATURAL

8.3.1 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).

- 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 concurran 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.

8.3.2 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 equivalente al restante para concluir el período originario de validez del certificado revocado.

- 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.

8.3.3 Procedimiento de Revocación

Solicitarán la revocación, llenando el formulario correspondiente en el portal de Certificación Electrónica, en cuanto tengan conocimiento de la concurrencia de alguna de las circunstancias contempladas en el apartado anterior:

- 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 el certificado.
- Compromiso de la fiabilidad del certificado.
- Compromiso de las claves.

En todo caso la ECIBCE podrá de oficio, iniciar el procedimiento de revocación de certificados, en cualquiera de los casos previstos en el apartado 8.3.1.

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 correo electrónico 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 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.

8.4 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 8.2.1.

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.

8.4.1 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 60 días calendario, antes de que transcurra la vigencia de su certificado y hasta 60 días calendario después.
- Que lo solicite en debido tiempo y forma, siguiendo las instrucciones y normas que la ECIBCE específica 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 8.2.3.

8.4.2 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 dirección correspondiente de 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, estos valores no le serán devueltos y no tendrá derecho a reclamo alguno.

c) 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.

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 al correo del solicitante/suscriptor registrado que debe realizar el pago.

e) 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 que se presente 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 del certificado y respectivamente a la firma del contrato de prestación del servicio y de la solicitud registrada.

8.5 VALIDEZ DEL CERTIFICADO DE FIRMA ELECTÓNICA 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.

8.6 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 dos días laborables para revisar el mismo, determinar si es adecuado y si los datos se corresponden con la realidad.

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

8.7 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 archivará una copia.

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