



## BANCO CENTRAL DEL ECUADOR

### Declaración de Prácticas de Certificación (DPC)

Instructivo de Gerencia IG-051-2010	Sustituye a:	Fecha de emisión: Junio de 2010	Fecha de revisión:	Página: 1/38
--	--------------	------------------------------------	--------------------	-----------------

#### 1. NORMAS GENERALES

##### 1.1. FINALIDAD

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

##### 1.2. APROBACIÓN

Gerencia General

##### 1.3. RESPONSABILIDAD DE LA EJECUCIÓN, DEL CONTROL PREVIO Y CONCURRENTES Y DE LA EVALUACIÓN DEL CONTROL INTERNO

Entidad de Certificación de Información.

##### 1.4 RESPONSABILIDAD DE LA EVALUACIÓN DEL CONTROL INTERNO

Auditoría General

##### 1.5 RESPONSABILIDAD DE LA REVISIÓN Y ACTUALIZACIÓN

Dirección de Entidad de Certificación de Información en coordinación con la Dirección de Desarrollo Organizacional.

##### 1.6 BASE LEGAL

Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos, su Reglamento; Ley Orgánica de Defensa del Consumidor, Ley Orgánica de Transparencia de la Información, Regulaciones Directorio Banco Central y Acreditación de CONATEL.

##### 1.7 VIGENCIA

El presente documento entrará en vigencia a partir de la fecha de su aprobación.

##### 1.8 DISTRIBUCIÓN

Responsables de la ejecución, Entidad de Certificación de Información y usuarios de Certificación de Firma electrónica.

##### 1.9 ÍNDICE



## BANCO CENTRAL DEL ECUADOR

### Declaración de Prácticas de Certificación (DPC)

Instructivo de Gerencia IG-051-2010	Sustituye a:	Fecha de emisión: Junio de 2010	Fecha de revisión:	Página: 2/38
--	--------------	------------------------------------	--------------------	-----------------

# ÍNDICE

NUMERAL	ASUNTO	PÁGINA
1.	NORMAS GENERALES .....	1
1.1.	FINALIDAD .....	1
1.2.	APROBACIÓN .....	1
1.3.	RESPONSABILIDAD DE LA EJECUCIÓN, DEL CONTROL PREVIO Y CONCURRENTE Y DE LA EVALUACIÓN DEL CONTROL INTERNO .....	1
1.5	RESPONSABILIDAD DE LA REVISIÓN Y ACTUALIZACIÓN .....	1
1.6	BASE LEGAL .....	1
1.7	VIGENCIA .....	1
1.8	DISTRIBUCIÓN .....	1
1.9	ÍNDICE .....	1
2	Soporte Legal .....	5
3	Resumen de la Declaración de Prácticas de Certificación (DPC) .....	6
3.1	Resumen .....	6
3.2	Garantía .....	6
3.3	Responsabilidad .....	6
3.4	Confidencialidad .....	6
3.5	Fuerza Mayor .....	6
3.6	Revocación del Certificado .....	7
3.7	Mantenimiento de Datos .....	7
3.8	Contenido del Certificado .....	7
3.9	Obligaciones del Suscriptor .....	7
3.10	Terceras partes .....	7
3.11	Legislación aplicable .....	7
3.12	Proceso de Resolución de Conflictos .....	8
	Declaración de Prácticas de Certificación de la Entidad de Certificación de Información del Banco Central del Ecuador .....	9
4	Introducción .....	10
4.1	Presentación .....	10
4.2	Definición y Acrónimos .....	10



# BANCO CENTRAL DEL ECUADOR

## Declaración de Prácticas de Certificación (DPC)

Instructivo de Gerencia IG-051-2010	Sustituye a:	Fecha de emisión: Junio de 2010	Fecha de revisión:	Página: 3/38
--	--------------	------------------------------------	--------------------	-----------------

4.3	Comunidad de usuarios y aplicabilidad .....	15
4.3.1	Autoridad de Certificación (AC) .....	15
4.3.2	Autoridad de Registro (AR) .....	15
4.3.3	Suscriptor .....	15
4.3.4	Solicitante .....	15
4.3.5	Usuario .....	15
4.4	Tipos de Certificados .....	15
4.4.1	Certificado de Firma Electrónica de Persona Natural .....	15
4.4.2	Certificado de Firma Electrónica de Persona Jurídica .....	16
4.4.3	Certificado de Firma Electrónica de Funcionario Público .....	16
4.5	Detalles de contacto .....	16
5	ASPECTOS GENERALES .....	17
5.1	Obligaciones .....	17
5.1.1	Obligaciones de la ECIBCE .....	17
5.1.2	Obligaciones de la AR .....	19
5.1.3	Obligaciones del Solicitante .....	19
5.1.4	Obligaciones del Suscriptor .....	20
5.1.5	Obligaciones de los Usuarios .....	20
5.1.5.1	Confianza en los certificados .....	21
5.2	Responsabilidades .....	22
5.2.1	Responsabilidades de la AC .....	22
5.2.2	Responsabilidades de la AR .....	22
5.2.3	Responsabilidades del Suscriptor .....	23
5.2.4	Responsabilidades del Usuario .....	23
5.3	Políticas de manejo de los Certificados de Firma Electrónica de la ECIBCE ..	23
5.4	Interpretación y ejecución .....	25
5.4.1	Ley aplicable .....	25
5.4.2	Subrogación y notificaciones .....	25
5.5	Procedimiento de resolución de conflictos .....	26
5.6	Tarifas de registro por la emisión y renovación de Certificados .....	26
5.7	Publicación y custodia .....	26
5.7.1	Publicación de información de la AC .....	26
5.8	Confidencialidad y protección de datos .....	27
5.8.1	Confidencialidad de las claves de firma electrónica .....	27



## BANCO CENTRAL DEL ECUADOR

### Declaración de Prácticas de Certificación (DPC)

Instructivo de Gerencia IG-051-2010	Sustituye a:	Fecha de emisión: Junio de 2010	Fecha de revisión:	Página: 4/38
--	--------------	------------------------------------	--------------------	-----------------

5.8.2	Confidencialidad en la prestación de servicios de certificación.....	27
5.9	Protección de datos .....	27
5.10	Derechos de propiedad intelectual.....	27
6	Gestión de las claves.....	28
6.1	De certificados de usuario final .....	28
6.2	Del certificado raíz de la AC .....	28
7	Solicitud de los servicios de Certificación .....	29
7.1	Emisión de Certificados.....	29
8	Revocación y suspensión de Certificados .....	30
8.1	Supuestos de revocación.....	30
8.1.1	Efectos de la revocación .....	30
8.2	Supuestos de suspensión.....	31
8.2.1	Efectos y límites de la Suspensión .....	31
8.3	Procedimiento de suspensión y revocación .....	31
8.3.1	Recepción de solicitudes de suspensión/revocación .....	32
8.3.2	Decisión de suspender/revocar .....	32
8.3.3	Comunicación y Publicación de la suspensión/revocación .....	32
9	Caducidad de Certificados.....	33
10	Renovación de los servicios de Certificación.....	33
10.1	Renovación de Certificados.....	33
11	Extinción de la AC .....	33
12	Características de los Certificados y de la lista de Certificados .....	34
12.1	Características de los Certificados.....	34
12.2	Lista de Certificados .....	35
12.3	Lista de Certificados Revocados (LCR).....	35
13	Controles de seguridad física, procedimental y de personal .....	36
14	Formatos .....	36
15	Otras cuestiones .....	36
15.1	Procedimientos modificación de la DPC y de las Prácticas de Certificación..	36
15.2	Procedimiento de publicación de las modificaciones.....	37
15.3	Procedimiento de notificación de las publicaciones.....	37



## BANCO CENTRAL DEL ECUADOR

### Declaración de Prácticas de Certificación (DPC)

Instructivo de Gerencia IG-051-2010	Sustituye a:	Fecha de emisión: Junio de 2010	Fecha de revisión:	Página: 5/38
--	--------------	------------------------------------	--------------------	-----------------

## 2 Soporte Legal

1. Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos, publicada en el Registro Oficial No. 577 de 17 de abril de 2002.

2. Reglamento General a la Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos, expedido mediante Decreto Ejecutivo No. 3496 publicado en el Registro Oficial 735 de 31 de diciembre de 2002, y reformas constantes en Decreto Ejecutivo 1356 de 29 de septiembre de 2008, publicadas en el Registro Oficial No.440 de 6 de octubre de 2008.

3. Segundo artículo enumerado agregado por el artículo 4 del Decreto Ejecutivo No.1356 a continuación del artículo 17 del Reglamento General a la Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos, dispone que la Acreditación como Entidad de Certificación de Información y Servicios Relacionados, consistirá en un acto administrativo emitido por el CONATEL, a través de una resolución que será inscrita en el Registro Público Nacional de Entidades de Certificación de Información y Servicios Relacionados Acreditadas y Terceros Vinculados.

4. Regulación No. 166-2008 de 3 de septiembre de 2008, publicada en el Registro Oficial No. 427 de 17 de septiembre de 2008, incorporó como Título XIII de la Codificación de Regulaciones de la Institución, "Del Servicio de Entidad de Certificación e Información y Emisión de Certificados de firma electrónica".

5. Resolución No. 481-20-CONATEL-2008 de 8 de octubre de 2008, aprobó la petición de Acreditación del Banco Central del Ecuador como Entidad de Certificación de Información y Servicios Relacionados, para lo cual la SENATEL suscribió el respectivo acto administrativo, conforme el modelo aprobado por el Consejo Nacional de Telecomunicaciones.

6. Regulación No. 169-2008 de 22 de octubre de 2008, mediante el cual el Directorio del Banco Central del Ecuador resolvió incorporar en el artículo 1, de la Sección II "El Banco Central del Ecuador", del Capítulo I (Tarifas, Tasas por Servicios y otros Conceptos relacionados con Operaciones Bancarias), del Título Séptimo (Tarifas y Tasas por Servicios) del Libro I (Política Monetaria – Crediticia) de la Codificación de Regulaciones del Banco Central del Ecuador, las tarifas que el Banco Central del Ecuador deberá cobrar a sus clientes, por la prestación de servicios en calidad de Entidad de Certificación de Información; y, sus reformas.



## BANCO CENTRAL DEL ECUADOR

### Declaración de Prácticas de Certificación (DPC)

Instructivo de Gerencia IG-051-2010	Sustituye a:	Fecha de emisión: Junio de 2010	Fecha de revisión:	Página: 6/38
--	--------------	------------------------------------	--------------------	-----------------

### 3 Resumen de la Declaración de Prácticas de Certificación (DPC)

#### 3.1 Resumen

ENTIDAD DE CERTIFICACIÓN DE INFORMACIÓN Y SERVICIOS RELACIONADOS (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. La ECIBCE será la encargada de la verificación de documentos e identificación de los solicitantes/suscriptores del certificado de firma electrónica y de completar el procedimiento definido para la emisión de certificados.

#### 3.2 Garantía

La ENTIDAD DE CERTIFICACIÓN DE INFORMACIÓN Y SERVICIOS RELACIONADOS, en adelante (ECIBCE) , sin perjuicio de la 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 es revocado si en cualquier momento la ECIBCE cree que los contenidos de un certificado no son correctos o que de cualquier manera la clave asociada a un certificado ha sido comprometida, manipulada o sea objeto de un 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.

#### 3.3 Responsabilidad

La ECIBCE acepta la responsabilidad directa e indirecta por cualquier negligencia en el desarrollo de sus prácticas de verificación. La ECIBCE no se hace responsable de los actos de terceras partes, suscriptores de certificados y de otras entidades ajenas a la ECIBCE.

#### 3.4 Confidencialidad

Los contenidos de los certificados emitidos por ECIBCE son información pública. La ECIBCE garantiza que no divulgará cualquier información adicional del suscriptor a ninguna tercera parte bajo ninguna razón, salvo la requerida por los tribunales siempre que éstos tengan jurisdicción para pedir una información específica.

#### 3.5 Fuerza Mayor

La ECIBCE no acepta ninguna responsabilidad por retraso o cualquier falta de cumplimiento de la presente Declaración de Prácticas de Certificación que resulten de eventos fuera de su control como casos de fuerza mayor, guerra, epidemia, terremoto,



## BANCO CENTRAL DEL ECUADOR

### Declaración de Prácticas de Certificación (DPC)

Instructivo de Gerencia IG-051-2010	Sustituye a:	Fecha de emisión: Junio de 2010	Fecha de revisión:	Página: 7/38
--	--------------	------------------------------------	--------------------	-----------------

incendio y cualquier otro evento que sea razonable de catalogar como de fuerza mayor.

#### 3.6 Revocación del Certificado

La ECIBCE podrá revocar o suspender certificados de acuerdo con las condiciones establecidas en esta DPC y publicará la lista de certificados revocados en una Lista de Certificados Revocados que sea pública y accesible.

#### 3.7 Mantenimiento de Datos

La ECIBCE mantendrá los datos y documentos relativos a la emisión de certificados por un plazo mínimo de 15 años, sin perjuicio del ejercicio del derecho de cancelación sobre los datos de carácter personal.

#### 3.8 Contenido del Certificado

Cada certificado emitido por la ECIBCE tiene por objeto el certificar únicamente la información contenida en el mismo. La ECIBCE no se hace responsable de ninguna asunción o interpretación relativa a información que no aparezca en el certificado.

Los datos que son almacenados en el certificado no contendrán tildes, ñ, diéresis, como política para la emisión de certificados.

#### 3.9 Obligaciones del Suscriptor

El suscriptor es el único responsable de la protección de sus claves privadas. Los suscriptores deberán notificar a la ECIBCE inmediatamente si creen que una clave privada ha sido o puede haber sido objeto de un mal uso de cualquier forma. Los suscriptores podrán ser responsables frente a la ECIBCE o frente a terceros de cualquier declaración incorrecta que hayan hecho a la ECIBCE, así como por cualquier consecuencia directa o indirecta derivada de aquéllas declaraciones incorrectas. Tanto los suscriptores como cualquiera que requiera de los servicios de certificación de la ECIBCE reconocen que han sido advertidos de que deben poseer una formación adecuada en el uso de los mecanismos de clave pública, previamente a pedir un certificado o tomar decisiones sobre la base del mismo. Los Suscriptores garantizan y responden, en cualquier caso, de la veracidad, exactitud, vigencia y autenticidad de los datos facilitados, y se comprometen a mantenerlos debidamente actualizados.

#### 3.10 Terceras partes

No se admitirán responsabilidades frente a terceros que se basen en un certificado 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.

#### 3.11 Legislación aplicable



## BANCO CENTRAL DEL ECUADOR

### Declaración de Prácticas de Certificación (DPC)

Instructivo de Gerencia IG-051-2010	Sustituye a:	Fecha de emisión: Junio de 2010	Fecha de revisión:	Página: 8/38
--	--------------	------------------------------------	--------------------	-----------------

Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos de 17 de Abril de 2002 y su Reglamento.

#### **3.12 Proceso 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 al vía del 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.



## BANCO CENTRAL DEL ECUADOR

### Declaración de Prácticas de Certificación (DPC)

Instructivo de Gerencia IG-051-2010	Sustituye a:	Fecha de emisión: Junio de 2010	Fecha de revisión:	Página: 9/38
--	--------------	------------------------------------	--------------------	-----------------

# Documento integro

## Declaración de Prácticas de Certificación de la Entidad de Certificación de Información del Banco Central del Ecuador

### Banco Central del Ecuador

Correo electrónico  
Dirección

Número de teléfono  
Número de Fax  
Casillero Postal  
Sitio Web

eci@bce.ec  
Av.10 de Agosto N11-409 y Briceño  
Quito - Ecuador  
(593-2) 2572522  
(593-2) 2289781  
339  
[www.bce.fin.ec](http://www.bce.fin.ec) sección Entidad de  
Certificación



## BANCO CENTRAL DEL ECUADOR

### Declaración de Prácticas de Certificación (DPC)

Instructivo de Gerencia IG-051-2010	Sustituye a:	Fecha de emisión: Junio de 2010	Fecha de revisión:	Página: 10/38
--	--------------	------------------------------------	--------------------	------------------

#### 4 Introducción

##### 4.1 Presentación

El presente documento constituye la Declaración de Prácticas de Certificación (DPC) de la ECIBCE, donde se definen los mecanismos relacionados con la práctica de certificación. Esta Declaración de Prácticas de Certificación (DPC) cumple con lo dispuesto en la Ley de Comercio Electrónico, Firmas Y Mensajes de Datos de la República del Ecuador.

La presente Declaración de Prácticas de Certificación (DPC) presenta las prácticas que la ECIBCE y sus Autoridades de Registro (AR) prestan en relación los servicios de certificación pública, 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. 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, como establece la legislación aplicable, las obligaciones legales y, proporciona información a todas las partes que crean, utilizan y validan certificados en el contexto de los 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 y las que emiten, gestionan, revocan y renuevan certificados en las DPC de la ECIBCE.

##### 4.2 Definición y Acrónimos

###### DEFINICIONES

**Acuerdo de Autoridad de Registro:** Contrato suscrito entre la ECIBCE y una determinada Dependencia del Banco Central del Ecuador, que tiene como objeto regular la relación jurídica entre ambos para una correcta comprobación de identidades para la emisión de Certificados Digitales por parte de la ECIBCE

**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 que emite certificados de firma electrónica y que puede prestar otros servicios relacionados con la firma electrónica

**Autoridad de Registro (AR):** Dependencia del Banco Central encargada de la comprobación de identidades para la emisión de Certificados Digitales por parte de la ECIBCE

**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.



## BANCO CENTRAL DEL ECUADOR

### Declaración de Prácticas de Certificación (DPC)

Instructivo de Gerencia IG-051-2010	Sustituye a:	Fecha de emisión: Junio de 2010	Fecha de revisión:	Página: 11/38
--	--------------	------------------------------------	--------------------	------------------

**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 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. Este certificado, puede ser utilizado por personas naturales, personas pertenecientes a empresas y funcionarios o servidores públicos.

**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.

**Clave pública:** Es la clave del certificado digital que se utiliza para la verificación de la firma electrónica y el cifrado de datos.

**Claves RSA:** Es el sistema criptográfico con clave pública RSA llamado así por sus creadores Ron Rivest, Adi Shamir y Len Adleman, 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.

**Contrato de Prestación de Servicios de Certificación:** Contrato que tiene por objeto regular los derechos y obligaciones derivados de la prestación por la ECIBCE, al suscriptor, de los servicios de Certificación, y, en su caso, la revocación y renovación, del mencionado servicio de Certificación.

**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.

**Dispositivo criptográfico portable seguro-Token:** Elemento físico donde se almacena en forma segura el certificado de firma electrónica que será emitido por la ECIBCE. Su uso es indispensable.

**DN 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, Pasaporte y demás documentos que la legislación Ecuatoriana admita como válidos para acreditar la identidad de una persona.

**Entidad de Certificación de información y servicios relacionados (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



## BANCO CENTRAL DEL ECUADOR

### Declaración de Prácticas de Certificación (DPC)

Instructivo de Gerencia IG-051-2010	Sustituye a:	Fecha de emisión: Junio de 2010	Fecha de revisión:	Página: 12/38
--	--------------	------------------------------------	--------------------	------------------

Nacional de Telecomunicaciones, según lo dispuesto en Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos y su Reglamento.

La ECIBCE será la encargada de la verificación de documentos e identificación de los solicitantes y suscriptores del certificado de firma electrónica y de completar el procedimiento definido para la emisión de certificados.

**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.

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

**Listado de Certificados Revocados (LCR):** Es una lista de certificados que han sido revocados, que no son válidos y en los que no debe confiar ningún usuario del sistema.

**Notario Público:** Persona encargada de emitir documentos públicos de acuerdo con las solemnidades requeridas por la legislación Ecuatoriana.

**OCSP:** Online Certificate Status Protocol (OCSP) es un método para determinar el estado de revocación de un certificado digital X.509 en línea.

**Persona física:** (o persona natural) concepto jurídico. Es todo ser humano susceptible de adquirir derechos y contraer obligaciones.

**Persona Jurídica:** Son entidades a las que el Derecho atribuye y reconoce una personalidad jurídica propia y, en consecuencia, capacidad para actuar como sujetos de derecho, esto es, capacidad para adquirir y poseer bienes de todas clases, para contraer obligaciones y ejercitar acciones judiciales.

**PKI:** En criptografía, una infraestructura de clave pública (o, en inglés, PKI, Public Key Infrastructure) 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.

**Políticas de Certificados (PC):** 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:** Persona física o 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.



## BANCO CENTRAL DEL ECUADOR

### Declaración de Prácticas de Certificación (DPC)

Instructivo de Gerencia IG-051-2010	Sustituye a:	Fecha de emisión: Junio de 2010	Fecha de revisión:	Página: 13/38
--	--------------	------------------------------------	--------------------	------------------

**Solicitante:** La persona natural, jurídica, funcionario o servidor público 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, jurídica o funcionario público 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 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

**Umbral límite (K,N) de SHAMIR** Esquemas criptográficos visuales secretos

**Usuario** La persona natural, persona jurídica, funcionario público que confía en un Certificado emitido por la ECIBCE.

**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

### ACRÓNIMOS

**AC:** Autoridad de Certificación

**AR:** Autoridad de Registro

**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** (Petición del certificado)

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

**DPC** Declaraciones de Prácticas de Certificación

**ECI:** Entidad de Certificación de Información

**ECIBCE:** Entidad de Información del Banco Central del Ecuador



## BANCO CENTRAL DEL ECUADOR

### Declaración de Prácticas de Certificación (DPC)

Instructivo de Gerencia IG-051-2010	Sustituye a:	Fecha de emisión: Junio de 2010	Fecha de revisión:	Página: 14/38
--	--------------	------------------------------------	--------------------	------------------

**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

**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)

**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.

**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.

**UTF8:** Unicode Transformation Format - 8 bits



## BANCO CENTRAL DEL ECUADOR

### Declaración de Prácticas de Certificación (DPC)

Instructivo de Gerencia IG-051-2010	Sustituye a:	Fecha de emisión: Junio de 2010	Fecha de revisión:	Página: 15/38
--	--------------	------------------------------------	--------------------	------------------

#### 4.3 Comunidad de usuarios y aplicabilidad

##### 4.3.1 Autoridad de Certificación (AC)

La ECIBCE actúa como Autoridad de Certificación (AC) relacionando 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.

##### 4.3.2 Autoridad de Registro (AR)

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

La ECIBCE podrá asignar la comprobación de identidades en una o varias oficinas del BCE que actúen como Autoridades de Registro. Las autoridades de registro comprobarán la identidad de los solicitantes de acuerdo con las normas de esta DPC, la PC y el acuerdo de AR. La relación con las Autoridades de Registro se rige por acuerdos específicos de prestación de servicios.

##### 4.3.3 Suscriptor

El suscriptor será la persona natural o funcionario privado o servidor público 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 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.

##### 4.3.4 Solicitante

A los efectos de esta DPC, se entenderá por Solicitante a la persona natural, jurídica, funcionario o servidor público 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.

##### 4.3.5 Usuario

Se entiende por Usuario del Certificado a la persona natural, jurídica, funcionario o servidor público que voluntariamente confía y hace uso de los Certificados de la ECIBCE. Cuando el Usuario decida voluntariamente confiar y hacer uso del Certificado le será de aplicación la presente DPC.

#### 4.4 Tipos de Certificados

##### 4.4.1 Certificado de Firma Electrónica de Persona Natural

Sirve para todo propósito, permite identificar a una persona natural, dentro del giro de sus negocios, y será responsable a título personal todo lo que firme, en forma electrónica, dentro del ámbito de su actividad y límites de su uso que correspondan.



## BANCO CENTRAL DEL ECUADOR

### Declaración de Prácticas de Certificación (DPC)

Instructivo de Gerencia IG-051-2010	Sustituye a:	Fecha de emisión: Junio de 2010	Fecha de revisión:	Página: 16/38
--	--------------	------------------------------------	--------------------	------------------

Las políticas referentes a este tipo de certificado se encuentran en la correspondiente PC.

#### 4.4.2 Certificado de Firma Electrónica de Persona Jurídica

Sirve para todo propósito, permite identificar a una persona jurídica de derecho privado, a través de su representante legal o de las personas que están perteneciendo a la empresa, quienes serán responsables en tal calidad de todo lo que firmen dentro del ámbito de su actividad y límites de uso que correspondan. Las políticas referentes a este tipo de certificado se encuentran en la correspondiente PC.

#### 4.4.3 Certificado de Firma Electrónica de Funcionario Público

Sirve para todo propósito, permite identificar a un funcionario o servidor público, quien será responsable a título de la institución pública 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 PC.

Sin perjuicio de las limitaciones de uso que se pudieran establecer, cabe la posibilidad de que se establezcan límites en el valor de las transacciones para las que puede utilizarse el certificado, con los mismos requisitos establecidos en la presente DPC para las limitaciones de uso.

En todo caso un certificado puede contener limitaciones de uso, o límites en el valor de las transacciones, o ambos aspectos, o ninguno de ellos.

#### 4.5 Detalles de contacto

Nombre	Banco Central del Ecuador
Nombre	o=eci, ou=bce, c=ec
Correo electrónico	eci@bce.ec
Dirección	Av.10 de Agosto N11-409 y Briceño
Número de teléfono	(593-2) 2572522
Número de Fax	(593-2) 2289781
Casillero Postal	339
Sitio Web	<a href="http://www.bce.fin.ec">www.bce.fin.ec</a> – Sección Entidad de Certificación

#### PERSONA DE CONTACTO

Nombre	Director de la Entidad de Certificación de Información del Banco Central del Ecuador
Correo electrónico	<a href="mailto:eci@bce.ec">eci@bce.ec</a>
Dirección	Av.10 de Agosto N11-409 y Briceño
Número de teléfono	(593-2) 2572522 Ext. 2221
Sitio Web	<a href="http://www.bce.fin.ec">www.bce.fin.ec</a> – Sección Entidad de Certificación



## BANCO CENTRAL DEL ECUADOR

### Declaración de Prácticas de Certificación (DPC)

Instructivo de Gerencia IG-051-2010	Sustituye a:	Fecha de emisión: Junio de 2010	Fecha de revisión:	Página: 17/38
--	--------------	------------------------------------	--------------------	------------------

## 5 ASPECTOS GENERALES

### 5.1 Obligaciones

#### 5.1.1 Obligaciones de la ECIBCE

- Emitir certificados conforme a esta DPC y a las PCs correspondientes y a los estándares de aplicación.
- 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 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 ajustándose según lo dispuesto en la 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 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.
- 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.
- Poner copias de sus propios certificados y de cualquier información de revocación a disposición de quien desee verificar una firma electrónica con referencia a dichos certificados, para lo cual publicará en su servidor web y en la CRL correspondiente [http://www.eci.bce.ec/CRL/eci\\_bce\\_ec\\_crlfile.crl](http://www.eci.bce.ec/CRL/eci_bce_ec_crlfile.crl) toda la información necesaria.
- Publicar los certificados emitidos 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.



## BANCO CENTRAL DEL ECUADOR

### Declaración de Prácticas de Certificación (DPC)

Instructivo de Gerencia IG-051-2010	Sustituye a:	Fecha de emisión: Junio de 2010	Fecha de revisión:	Página: 18/38
--	--------------	------------------------------------	--------------------	------------------

- 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 Subscriptores y AR's que estén vinculadas a ella.
- Cumplir las obligaciones de la presente DPC
- Todas aquellas obligaciones impuestas por la presente DPC y, en su caso, la Ley de Comercio Electrónico, Firmas electrónicas y Mensajes de datos.
- Ofrecer y mantener la infraestructura tecnológica necesaria para el establecimiento de una estructura, tanto en hardware como en software, para operar 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) y en las Políticas de Certificados.
- Poner a disposición de los usuarios el listado de certificados revocados (LCR), a través de la página Web [http://www.eci.bce.ec/CRL/eci\\_bce\\_ec\\_crlfile.crl](http://www.eci.bce.ec/CRL/eci_bce_ec_crlfile.crl).
- Comunicar de manera inmediata a los titulares de los certificados emitidos por ésta, el compromiso de su clave privada, pérdida, divulgación, modificación, uso no autorizado, con el fin de revocarlos.



## BANCO CENTRAL DEL ECUADOR

### Declaración de Prácticas de Certificación (DPC)

Instructivo de Gerencia IG-051-2010	Sustituye a:	Fecha de emisión: Junio de 2010	Fecha de revisión:	Página: 19/38
--	--------------	------------------------------------	--------------------	------------------

- 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; y,
- Proteger los datos personales de los solicitantes y usuarios de certificados digitales o electrónicos.

#### 5.1.2 Obligaciones de la AR

- La AR podrá asumir las siguientes obligaciones de las cuales será responsable.
- Identificar y autenticar correctamente al Suscriptor y/o Solicitante y/o a la organización que represente, conforme a los procedimientos que se establecen en esta DPC y en las Prácticas de Certificación específicas para cada tipo de Certificado, utilizando cualquiera de los medios admitidos en derecho.
- Formalizar los contratos de expedición de los certificados con el Suscriptor en los términos y condiciones que establezca la AC.
- Almacenar de forma segura y por un periodo nunca inferior a 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 para la Autoridad de Registro.
- Llevar a cabo cualesquiera otras funciones 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 para Autoridad de Registro.
- En todo caso, la AR permitirá a ECIBCE el acceso a los archivos y 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.
- 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.

#### 5.1.3 Obligaciones del Solicitante

- Abonar las tarifas de registro que correspondan en virtud de los servicios que se soliciten.



## BANCO CENTRAL DEL ECUADOR

### Declaración de Prácticas de Certificación (DPC)

Instructivo de Gerencia IG-051-2010	Sustituye a:	Fecha de emisión: Junio de 2010	Fecha de revisión:	Página: 20/38
--	--------------	------------------------------------	--------------------	------------------

- Suministrar a la AR la información necesaria para realizar una correcta identificación.
- Confirmar la exactitud y veracidad de la información suministrada.
- Notificar cualquier cambio en los datos aportados para la creación del certificado durante su periodo de validez.
- Solicitar el Certificado según se estipula en los términos y condiciones que se establezcan en la PC de cada tipo de Certificados y, en su caso, en el Contrato para la prestación de servicios de certificados suscrito con la ECIBCE.

#### 5.1.4 Obligaciones del Suscriptor

- Cumplir en todo momento con las normas y regulaciones emitidas por el Banco Central y la ECIBCE en su DPC y las correspondientes Políticas de Certificados.
- Comunicar a la ECIBCE cualquier modificación o variación de los datos que se aportaron para obtener el Certificado de Firma Electrónica.
- Verificar, a través de la Lista de Certificados Revocados, el estado de los Certificados de firma electrónica.
- Proteger y conservar el Dispositivo Portable Seguro-Token.
- Solicitar la revocación del certificado y la emisión de uno nuevo a la ECIBCE, en caso de olvido de la clave de protección del Certificado de Firma Electrónica.
- Responder por el uso del Certificado de Firma Electrónica y de las consecuencias que se deriven de su utilización.
- Cumplir con lo estipulado en el artículo 17 de la Ley de Comercio Electrónico, Firmas Electrónicas y Mensaje de Datos.

#### 5.1.5 Obligaciones de los Usuarios

- Los Usuarios que pretendan confiar y usar los Certificados emitidos por la AC deberán verificar la validez de las firmas emitidas por los Suscriptores.
- En el supuesto de que los Usuarios no procedieran a verificar las firmas a través de la CRL (Lista de Certificados revocados), la ECIBCE no se hace responsable del uso y confianza que los Usuarios hagan de estos Certificados.
- Toda persona tendrá derecho a confiar en una firma electrónica emitida mediante un Certificado de la ECIBCE en la medida en que sea razonable hacerlo.



## BANCO CENTRAL DEL ECUADOR

### Declaración de Prácticas de Certificación (DPC)

Instructivo de Gerencia IG-051-2010	Sustituye a:	Fecha de emisión: Junio de 2010	Fecha de revisión:	Página: 21/38
--	--------------	------------------------------------	--------------------	------------------

- Para determinar si es razonable confiar, deberá tenerse en cuenta, en su caso, lo siguiente:
- La naturaleza de la operación correspondiente que la firma tenga por objeto avalar. No se considerará razonable confiar en una firma emitida por un certificado de la ECIBCE si dicha operación puede ser considerada un uso indebido.
- Si la parte que confía ha adoptado las medidas adecuadas para determinar la fiabilidad de la firma, y en particular, si ha verificado que el certificado no esté caducado, suspendido o revocado. La caducidad constará en el propio Certificado. La posible suspensión o revocación del Certificado deberán ser consultadas en la lista de revocaciones o suspensiones de certificados (CRL).
- Si la parte que confía sabía o debía haber sabido que la firma estaba en entredicho o había sido revocada o suspendida.
- 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 distinto.

#### 5.1.5.1 Confianza en los certificados

Toda persona tendrá derecho a confiar en un Certificado de la ECIBCE en la medida en que sea razonable hacerlo.

Para determinar si es razonable confiar, 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, (CRL);
- 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 distinto.
- Todo otro factor pertinente.
- 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, establecidas por contrato, dentro de los cuales se asegura la prestación de los servicios de certificación.



## BANCO CENTRAL DEL ECUADOR

### Declaración de Prácticas de Certificación (DPC)

Instructivo de Gerencia IG-051-2010	Sustituye a:	Fecha de emisión: Junio de 2010	Fecha de revisión:	Página: 22/38
--	--------------	------------------------------------	--------------------	------------------

## 5.2 Responsabilidades

### 5.2.1 Responsabilidades de la AC

- Garantizar el cumplimiento de las responsabilidades y obligaciones descritas en esta DPC; y lo previsto en la Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos, y su Reglamento.
- 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 y 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 por ella emitidos en favor de un determinado suscriptor.
- La ECIBCE no será responsable de las eventuales inexactitudes en el Certificado que resulten de la información facilitada por el Suscriptor, 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 PCs 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 un supuesto 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 electrónicos firmados digitalmente. Ni la ECIBCE ni sus autoridades de registro serán responsables en ningún caso por los daños causados por el empleo de sus servicios de certificación pública en estos entornos.

### 5.2.2 Responsabilidades de la AR

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



## BANCO CENTRAL DEL ECUADOR

### Declaración de Prácticas de Certificación (DPC)

Instructivo de Gerencia IG-051-2010	Sustituye a:	Fecha de emisión: Junio de 2010	Fecha de revisión:	Página: 23/38
--	--------------	------------------------------------	--------------------	------------------

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 las presentes DPC y en las PC 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.

#### 5.2.3 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, y por la normativa vigente en materia de prestación de servicios de certificación.
- El Suscriptor se compromete a indemnizar a la ECIBCE 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 cumplimiento 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.

#### 5.2.4 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.
- En todo caso, el Usuario asumirá toda la responsabilidad y riesgos derivados de la aceptación de un Certificado 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.

### 5.3 Políticas de manejo de los Certificados de Firma Electrónica de la ECIBCE



## BANCO CENTRAL DEL ECUADOR

### Declaración de Prácticas de Certificación (DPC)

Instructivo de Gerencia IG-051-2010	Sustituye a:	Fecha de emisión: Junio de 2010	Fecha de revisión:	Página: 24/38
--	--------------	------------------------------------	--------------------	------------------

- 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 un uso indebido de un Certificado cuando éste sea utilizado para realizar operaciones no autorizadas según las Políticas de Certificados aplicables a cada uno de los Certificados, y los Contratos de la ECIBCE con sus suscriptores, consecuencia de esto la ECIBCE podrá revocar el certificado y dar por terminado el contrato.
- Los usos autorizados de los Certificados emitidos por la ECIBCE pueden estar especificados en cada tipo de certificado.
- Si el certificado del suscriptor en el período de vigencia se encontrara comprometido, es decir su clave privada, deberá iniciar el procedimiento de revocación como se lo menciona en esta DPC, y en las PC.

El certificado de firma electrónica emitido por la ECIBCE al suscriptor, deberá ser utilizado tal y como son suministrados. Queda prohibido 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.
- Los certificados de firma electrónica presentan las siguientes garantías:
  - Autenticidad. La información del documento y su firma electrónica se corresponden indubitablemente 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.- La información contenida ha sido cifrada y por voluntad del emisor, solo permite que el receptor pueda descifrarla.

#### IMPORTANTE

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 del usuario.

El uso de claves públicas contenidas en un certificado pueden ser utilizadas 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 privada el mensaje simplemente no se podrá descifrar por ningún medio.

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



## BANCO CENTRAL DEL ECUADOR

### Declaración de Prácticas de Certificación (DPC)

Instructivo de Gerencia IG-051-2010	Sustituye a:	Fecha de emisión: Junio de 2010	Fecha de revisión:	Página: 25/38
--	--------------	------------------------------------	--------------------	------------------

#### 5.4 Interpretación y ejecución

##### 5.4.1 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.

##### 5.4.2 Subrogación y notificaciones

La ECIBCE se reserva el derecho de transmitir en el futuro todas las obligaciones y derechos que se deriven de esta DPC a un tercero para que éste continúe prestando el servicio de certificación. Ante esta hipotética Subrogación de la AC de la ECIBCE realizará todas las gestiones necesarias para obtener el consentimiento expreso de los subscriptores, antes de transferir la gestión de los certificados, que sigan en vigor en la fecha en que se produzca la subrogación, a otro prestador de servicios de certificación o, en caso contrario, extinguir la vigencia de los certificados. Para la consecución de estos objetivos se establecen las siguientes medidas:

Esta DPC seguirá siendo el documento que regule las relaciones entre las partes mientras no se cree un nuevo documento por escrito.

Comunicará fehacientemente, al Organismo de Control y con una antelación mínima de tres meses la subrogación de la actividad, informando al mismo tiempo sobre todas las características del Prestador de Servicios de Certificación al que se propone la transferencia de la gestión de los certificados.

Recabar el consentimiento expreso de los suscriptores que tengan en ese momento certificado esté en vigor para la transferencia de la gestión de los certificados.

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 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 resolución.

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.

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.



## BANCO CENTRAL DEL ECUADOR

### Declaración de Prácticas de Certificación (DPC)

Instructivo de Gerencia IG-051-2010	Sustituye a:	Fecha de emisión: Junio de 2010	Fecha de revisión:	Página: 26/38
--	--------------	------------------------------------	--------------------	------------------

Cualquier otra obligación que venga impuesta por la ley.

#### 5.5 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 al vía del 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.

#### 5.6 Tarifas de registro por la emisión y renovación de Certificados

Las tarifas de registro vigentes en cada momento por la emisión y renovación de Certificados serán puestas a disposición de los Solicitantes por la Autoridad de Certificación en la página web [www.bce.fin.ec](http://www.bce.fin.ec). Las tarifas de registro son reguladas mediante resoluciones del Banco Central del Ecuador.

#### 5.7 Publicación y custodia

##### 5.7.1 Publicación de información de la AC

El contenido de esta DPC, así como de toda la información que se publique, estará expuesta a título informativo en la dirección de Internet: <http://www.bce.fin.ec> Sección Entidad de Certificación - DeclaracionesPracticasCertificacion.pdf y los originales estarán custodiados en las oficinas de la AC.

Igualmente, tanto los Usuarios como los Solicitantes / Suscriptores podrán tener acceso de forma fiable a la información de la AC dirigiéndose a sus oficinas o a las de



## BANCO CENTRAL DEL ECUADOR

### Declaración de Prácticas de Certificación (DPC)

Instructivo de Gerencia IG-051-2010	Sustituye a:	Fecha de emisión: Junio de 2010	Fecha de revisión:	Página: 27/38
--	--------------	------------------------------------	--------------------	------------------

cualquier AR, o bien, solicitándolo a la dirección de correo [eci@bce.ec](mailto:eci@bce.ec) a través de la cual se remitirá la información firmada con un Certificado de la ECIBCE.

#### **5.8 Confidencialidad y protección de datos**

##### **5.8.1 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 clientes o que las Autoridades Certificadoras de Segundo Nivel encadenadas con la ECIBCE proporcionan a sus clientes. Asimismo, una vez generadas y entregadas las claves privadas, la AC se abstendrá de almacenar, copiar o conservar cualquier tipo de información que sea suficiente para reconstruir dichas claves.

##### **5.8.2 Confidencialidad en la prestación de servicios de certificación**

Tanto la AC como las AR 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.

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

#### **5.9 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 bajo la responsabilidad de la ECIBCE, 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 acciones previstas 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 los datos de carácter personal contenidos en el archivo, requerirá previo consentimiento del Suscriptor / Solicitante. Asimismo, se informa sobre el derecho que asiste al Suscriptor para acceder, rectificar o cancelar sus datos de carácter personal, en los términos recogidos por la normativa sobre tratamiento de datos de carácter personal.

#### **5.10 Derechos de propiedad intelectual**

La ECIBCE es titular en exclusiva de todos los derechos de propiedad intelectual que puedan derivarse del sistema de certificación que regula esta DPC. Se prohíbe por tanto, cualquier acto de reproducción, distribución, comunicación pública y



## BANCO CENTRAL DEL ECUADOR

### Declaración de Prácticas de Certificación (DPC)

Instructivo de Gerencia IG-051-2010	Sustituye a:	Fecha de emisión: Junio de 2010	Fecha de revisión:	Página: 28/38
--	--------------	------------------------------------	--------------------	------------------

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 Certificado cuando la misma sea necesaria para la utilización del Certificado por parte del usuario legítimo y con arreglo a la finalidad del Certificado, 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.

## 6 Gestión de las claves

### 6.1 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, como prestador de servicios de certificación. Estas normas o estándares son los siguientes:

- El tamaño de las claves será como mínimo de 1024 bits.
- El algoritmo utilizado para la generación de las claves es el RSA.
- La generación de la función resumen (HASH) se realiza utilizando el algoritmo SHA1 de 160 bits.
- El período de validez de las claves va a ser, como máximo, de dos años desde que se emite o renueva el Certificado, o el máximo establecido por la legislación vigente.

### 6.2 Del certificado raíz de la AC

Las claves de la AC se han mantenido depositadas custodiadas en un sistema seguro. El acceso a esas claves sólo se permite a personas debidamente autorizadas por la ECIBCE.

En su caso, si en algún momento se viera en la necesidad de la eliminación de las claves, el procedimiento que se seguirá será el de sobre escritura.

- El tamaño de las claves es de 2048 bits.
- El algoritmo utilizado para la generación de las claves es el RSA.
- La generación de la función resumen (HASH) se realiza utilizando el algoritmo SHA1 de 160 bits.
- El período de validez de las claves es como máximo, de veinte años

Contenido del certificado raíz de la ECIBCE

CAMPO	DESCRIPCION
<i>Versión</i>	<i>Versión del certificado estándar X509</i>
<i>Número de serie</i>	<i>Numero de serie del certificado</i>
<i>Algoritmo de firma</i>	<i>RSA SHA 1</i>
<i>Emisor</i>	<i>Datos de la ECIBCE</i>
<i>Valido desde</i>	<i>Fecha de emisión</i>
<i>Valido hasta</i>	<i>Fecha de caducidad</i>
<i>Asunto</i>	<i>Datos de la ECIBCE</i>



## BANCO CENTRAL DEL ECUADOR

### Declaración de Prácticas de Certificación (DPC)

Instructivo de Gerencia IG-051-2010	Sustituye a:	Fecha de emisión: Junio de 2010	Fecha de revisión:	Página: 29/38
--	--------------	------------------------------------	--------------------	------------------

<i>Clave Pública</i>	<i>Clave Pública de la ECIBCE</i>
<i>Tipo de certificado Netscape</i>	<i>Extensión no crítica del estándar X509</i>
<i>Puntos de distribución</i>	<i>Puntos de distribución de CRL. Dirección donde se publica la lista de revocación de Certificados</i>
<i>Periodo de uso de clave privada</i>	<i>Periodo dentro del cual es válida la clave privada</i>
<i>Uso de clave</i>	<i>Identifica el uso que será aplicable</i>
<i>Identificador de clave de entidad emisora</i>	<i>Extensión del estándar X509</i>
<i>Identificador de clave de asunto</i>	<i>Extensión del estándar X509</i>
<i>Restricciones Básicas</i>	<i>Determina a que está destinada la AC, y la ruta de certificación como entidad final de ECIBCE</i>
<i>Algoritmo de identificación</i>	<i>Algoritmo de firma utilizado por la AC</i>
<i>Huella digital</i>	<i>Id de huella asociado al certificado</i>

## 7 Solicitud de los servicios de Certificación

### 7.1 Emisión de Certificados

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 tendrá la potestad de aprobar o no la emisión. Aprobada la emisión, el solicitante efectuará el pago de la tarifa respectiva.

Una vez realizado el pago, el solicitante será notificado para que acuda a la ECIBCE en fecha y hora para proceder a la identificación y emisión del certificado solicitado.

El solicitante/suscriptor deberá presentarse ante la Autoridad de Registro de la ECIBCE con una cédula de ciudadanía válida y suficientemente clara y actualizada para permitir su inequívoca identificación y los originales del resto de la documentación solicitada; suscribirá 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.

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.



## BANCO CENTRAL DEL ECUADOR

### Declaración de Prácticas de Certificación (DPC)

Instructivo de Gerencia IG-051-2010	Sustituye a:	Fecha de emisión: Junio de 2010	Fecha de revisión:	Página: 30/38
--	--------------	------------------------------------	--------------------	------------------

## 8 Revocación y suspensión de Certificados

### 8.1 Supuestos de revocación

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

- Solicitud voluntaria del Suscriptor.
- Solicitud voluntaria del Solicitante.
- Pérdida o inutilización por daños del soporte del certificado.
- Fallecimiento del suscriptor, incapacidad sobrevenida, total o parcial, de cualquiera de ellos, 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 graves 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 resolución del contrato
- 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.
- Por la concurrencia de cualquier otra causa especificada en la presente DPC o en las correspondientes Prácticas de Certificación establecidas para cada tipo de Certificado.

#### 8.1.1 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.



## BANCO CENTRAL DEL ECUADOR

### Declaración de Prácticas de Certificación (DPC)

Instructivo de Gerencia IG-051-2010	Sustituye a:	Fecha de emisión: Junio de 2010	Fecha de revisión:	Página: 31/38
--	--------------	------------------------------------	--------------------	------------------

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.

#### 8.2 Supuestos de suspensión

El certificado podrá ser suspendido cuando existan indicios sobre la existencia de una causa de revocación. En la actualidad no se está proporcionando el servicio de suspensión debido a condicionantes técnicos, aunque se admite en esta DPC a efectos de servicio futuro.

##### 8.2.1 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 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 revocar 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.

#### 8.3 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 hayan participado.
- La persona jurídica que conste en el Certificado.

Asimismo, podrá solicitar la suspensión/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 signatario.
- Incapacidad sobrevenida, total o parcial.
- Inexactitudes en el certificado.
- Compromiso de la fiabilidad del Certificado.
- Compromiso de las claves.
- Cese del representante en el caso de los certificados con poderes.
- Extinción de la persona jurídica representada.



## BANCO CENTRAL DEL ECUADOR

### Declaración de Prácticas de Certificación (DPC)

Instructivo de Gerencia IG-051-2010	Sustituye a:	Fecha de emisión: Junio de 2010	Fecha de revisión:	Página: 32/38
--	--------------	------------------------------------	--------------------	------------------

- Revocación de la autorización de la entidad que conste en el Certificado en el caso de los Certificados sin poderes.

En todo caso, la AC 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.

#### 8.3.1 Recepción de solicitudes de suspensión/revocación

La solicitud de suspensión/revocación de Certificados se podrá dirigir a la AC en la forma de comunicación escrita o digital, o presentándose físicamente ante la ECIBCE

Aquel Solicitante/Suscriptor que solicite la suspensión/revocación deberá solicitarla mediante el formulario respectivo de revocación disponible en la página del portal Web de la ECIBCE.

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 o Funcionario Público, y en caso de Persona Natural podrá gestionar de manera presencial una persona de confianza para validar el proceso.

#### 8.3.2 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 AC.

#### 8.3.3 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 LCR. La publicación de las CRL's realizará cada 24 horas o cada vez que se revoca un certificado.

Su consulta se puede realizar vía web en:

[http://www.eci.bce.ec/crl/eci\\_bce\\_ec\\_crlfile.crl](http://www.eci.bce.ec/crl/eci_bce_ec_crlfile.crl)

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 indicación 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. En caso de fallo del sistema, servicio o cualquier otro



## BANCO CENTRAL DEL ECUADOR

### Declaración de Prácticas de Certificación (DPC)

Instructivo de Gerencia IG-051-2010	Sustituye a:	Fecha de emisión: Junio de 2010	Fecha de revisión:	Página: 33/38
--	--------------	------------------------------------	--------------------	------------------

factor que no esté bajo el control de la ECIBCE, la ECIBCE deberá realizar los esfuerzos que razonablemente estén a su alcance para confirmar que este servicio de información no se encuentre indisponible durante más tiempo que el periodo máximo dispuesto en esta política.

#### 9 Caducidad de Certificados

Los Certificados caducarán por el transcurso del período operacional 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.

#### 10 Renovación de los servicios de Certificación.

##### 10.1 Renovación de Certificados

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

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

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

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.

#### 11 Extinción de la AC

En orden a causar el menor daño posible tanto a los Suscriptores como a los Usuarios del sistema de certificación ante un hipotético cese de la ECIBCE

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



## BANCO CENTRAL DEL ECUADOR

### Declaración de Prácticas de Certificación (DPC)

Instructivo de Gerencia IG-051-2010	Sustituye a:	Fecha de emisión: Junio de 2010	Fecha de revisión:	Página: 34/38
--	--------------	------------------------------------	--------------------	------------------

- Establecer, cuando ello fuera posible, un acuerdo con otro Prestador del Servicio de Certificación con el propósito de transmitir todas sus obligaciones y derechos dentro del sistema de certificación con la intención de continuar el servicio. Si se produce la subrogación, esta DPC seguirá siendo el documento que establece las relaciones entre las partes mientras no se establezca un nuevo documento por escrito. Comunicará fehacientemente al Organismo de Control y con una antelación mínima de tres meses el cese de la actividad, informando al mismo tiempo sobre todas las características del Prestador de Servicios de Certificación al que se propone la transferencia de la gestión de los certificados.
- 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.
- 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 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 resolución.
- Informar a las administraciones 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 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
- Cualquier otra obligación que venga impuesta por la ley.

## 12 Características de los Certificados y de la lista de Certificados

### 12.1 Características de los Certificados

Los certificados emitidos por la ECIBE serán almacenados en un dispositivo criptográfico (TOKEN), manteniendo niveles y estándares de seguridad. Los dispositivos serán entregados de manera personal al suscriptor por parte de la AC o AR de la ECIBCE.

Los certificados de usuario final tiene una vigencia de 2 años, mientras que la vigencia del certificado raíz es de veinte años



## BANCO CENTRAL DEL ECUADOR

### Declaración de Prácticas de Certificación (DPC)

Instructivo de Gerencia IG-051-2010	Sustituye a:	Fecha de emisión: Junio de 2010	Fecha de revisión:	Página: 35/38
--	--------------	------------------------------------	--------------------	------------------

#### 12.2 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.

El Listado de Certificados estará a disposición de los usuarios en la página web de la ECIBCE. El Listado de Certificados suspendidos o revocados (CRL) estará a disposición de los usuarios en la página:

[http://www.eci.bce.ec/crl/eci\\_bce\\_ec\\_crlfile.crl](http://www.eci.bce.ec/crl/eci_bce_ec_crlfile.crl)

Los Certificados suspendidos y revocados aparecerán como tales en la CRL durante un período mínimo de tres años, a partir del cual se eliminará los datos del Certificado definitivamente de la CRL y serán depositados en las oficinas de la AC durante un periodo de doce años.

#### 12.3 Lista de Certificados Revocados (LCR)

El Banco Central del Ecuador, a través de 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 Estatus de Certificados en Línea (OCSP), URL: <http://ocsp.eci.bce.ec>, para que de esta manera sea fácilmente accesible por los usuarios.

La ECIBCE mantiene publicada la Lista de Certificados Revocados con una periodicidad de cada 6 horas por 14 horas al día, es decir se hará pública la CRL 3 veces al día para que los usuarios puedan acceder a la verificación. Hay que recalcar que la ECIBCE mantiene en línea la verificación del estado de un certificado mediante un repositorio LDAP, es decir, una vez revocado un certificado, inmediatamente al proceder a firmar un documento o mensaje de datos, le mostrará un mensaje indicando que el certificado se encuentra revocado.

Las CRL's generadas por la ECIBCE tiene un tiempo de vigencia 24 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.

El Banco Central del Ecuador, a través de la Entidad de Certificación de Información, mantendrá actualizada la LCR y la OCSP (en cuanto este servicio esté disponible), incluyendo todos los certificados revocados desde la última actualización.

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

CAMPO	DESCRIPCION
<i>Versión</i>	<i>Versión de la lista</i>
<i>Emisor</i>	<i>Entidad de Certificación Emisora</i>
<i>Fecha efectiva</i>	<i>Fecha de publicación</i>
<i>Próxima actualización</i>	<i>Fecha de vencimiento</i>
<i>Algoritmo de firma</i>	<i>Algoritmo utilizado</i>



## BANCO CENTRAL DEL ECUADOR

### Declaración de Prácticas de Certificación (DPC)

Instructivo de Gerencia IG-051-2010	Sustituye a:	Fecha de emisión: Junio de 2010	Fecha de revisión:	Página: 36/38
--	--------------	------------------------------------	--------------------	------------------

<i>Número CRL</i>	<i>Número de revocaciones</i>
<i>Identificador de clave de entidad emisora</i>	<i>Id de clave</i>

### 13 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. Está descrito en el documento “Declaración de Políticas de Seguridad”.

### 14 Formatos

La Lista de Certificados Revocados (LCR), se encuentra disponible en formato LRC V2, en el repositorio de la Entidad de Certificación de Información del Banco Central del Ecuador.

Las Políticas de Certificados de la Entidad de Certificación de Información del Banco Central del Ecuador, se podrán ubicar 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 la base de datos pública.

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, bien realizando la solicitud correspondiente a través del siguiente número de teléfono: +593-22572522 ext 2743.

### 15 Otras cuestiones

#### 15.1 Procedimientos de modificación de la DPC y de las Prácticas de Certificación

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



## BANCO CENTRAL DEL ECUADOR

### Declaración de Prácticas de Certificación (DPC)

Instructivo de Gerencia IG-051-2010	Sustituye a:	Fecha de emisión: Junio de 2010	Fecha de revisión:	Página: 37/38
--	--------------	------------------------------------	--------------------	------------------

#### 15.2 Procedimiento de publicación de las modificaciones

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

#### 15.3 Procedimiento de notificación de las publicaciones

En caso que las modificaciones efectuadas en la DPC incidan directamente en los derechos y obligaciones de los Suscriptores y/o Solicitantes, así como cuando dichas modificaciones alteren la operatividad de los Certificados por parte de los usuarios, deberán notificarse dichas modificaciones a los Suscriptores y/o Solicitantes con un período de antelación de quince días 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 modificaciones implicará su aceptación. La no aceptación de las modificaciones de esta DPC realizadas por la AC, tendrá como consecuencia la resolución de contrato con el suscriptor/solicitante.

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

**Aprobado por:**

**Fecha: 1 de julio de 2010**

Ing. Christian Ruiz H.; MA  
**Gerente General**



## BANCO CENTRAL DEL ECUADOR

### Declaración de Prácticas de Certificación (DPC)

Instructivo de Gerencia IG-051-2010	Sustituye a:	Fecha de emisión: Junio de 2010	Fecha de revisión:	Página: 38/38
--	--------------	------------------------------------	--------------------	------------------

**Elaborado por:**

Ing. Xavier Pazos  
**Dirección de Entidad de Certificación**

Ing. Hernán González  
**Director de Entidad de Certificación**

**Revisado por:**

Econ. Verónica Legarda  
**Subgerente General**

Ing. Diego Calderón  
**Director de Desarrollo Organizacional**

Lcda. Catalina Oviedo  
**Dirección de Desarrollo Organizacional**

**Auditoría General**, conforme se desprende de oficio No. AU-C-240-2010 de 31 de mayo de 2010.

**Asesoría Legal**, conforme se desprende de oficio No. AL-DEB-378-I de 11 de mayo de 2010.