ENTIDAD DE CERTIFICACIÓN DEL CONSEJO DE LA JUDICATURA

ICERT-EC

POLÍTICA DE CERTIFICADOS

Certificado de Departamento de Empresa o Institución

ICERT - EC ENTIDAD DE CERTIFICACIÓN Consejo de la Judicatura	***POLÍTICA DE CERTIFICADOS DE DEPARTAMENTO DE EMPRESA O INSTITUCIÓN***	*Versión: 3.0*
		Fecha: 09-08-2016
		OID: 1.3.6.1.4.1.437451.2.3.1

Código:	Sustituye a:	Fecha de emisión:	Fecha de revisión:
00-11-A.05-POL3.0-7Política de Certificados de Departamento de Empresa o Institución	00-11-A.05-POL2.0-7Política de Certificados de Departamento de Empresa o Institución	Octubre 2014	Septiembre 2016

Historial de modificaciones

Fecha	Versión	Creado por	Descripción de la modificación
2014-06-02	1.0	**CONSEJO DE LA JUDICATURA** David Moncayo	
2014-10-17	2.0	**CONSEJO DE LA JUDICATURA** David Moncayo Flor Chancay	Se realizó actualización de la documentación presentada ante SENATEL para obtener la acreditación.
2016-09-08	3.0	**CONSEJO DE LA JUDICATURA** David Moncayo Flor Chancay	Se introducen cambios según Acuerdo MINTEL 012-2016 de 23 de mayo de 2016. Se realizó actualización de roles y proceso de solicitud y emisión de certificados.

Firmas de responsabilidad

	Nombre	Cargo	Firma
Creado por:	David Moncayo	Jefe de Unidad	
Creado por:	Flor Chancay	Analista 2	
Revisado por:	Reynaldo Gaibor	Subdirector Nacional de Seguridad de la Información	
Aprobado por:	Tomás Alvear	Director General	

Código:	Sustituye a:	Fecha de emisión:	Fecha de revisión:
00-11-A.05-POL3.0-7Política de Certificados de Departamento de Empresa o Institución	00-11-A.05-POL2.0-7Política de Certificados de Departamento de Empresa o Institución	Octubre 2014	Septiembre 2016

CONTENIDO

Código:	Sustituye a:	Fecha de emisión:	Fecha de revisión:
00-11-A.05-POL3.0-7Política de Certificados de Departamento de Empresa o Institución	00-11-A.05-POL2.0-7Política de Certificados de Departamento de Empresa o Institución	Octubre 2014	Septiembre 2016

1. INTRODUCCIÓN

El Consejo de la Judicatura en su calidad de órgano de Gobierno, administración, vigilancia y disciplina de la Función Judicial, con el objetivo de estandarizar los procedimientos internos de uso de Certificados Digitales, disminuir costos relacionados con la operación de Sistemas Informáticos y Seguridad de la Información, así como emisión de certificados electrónicos para toda la Función Judicial; implementó la Infraestructura de Clave Pública (PKI).

A través del Decreto Ejecutivo No. 867 de 1 de septiembre de 2011, se expide la siguiente reforma al Reglamento General A La Ley De Comercio Electrónico, Firmas Electrónicas y Mensajes De Datos.

> *"Artículo 1.- Sustituir el undécimo artículo innumerado agregado a continuación del artículo 17, referente a la Acreditación para Entidades del Estado, con el siguiente texto:*
>
> *"Acreditación para Entidades del Estado.- Las instituciones y entidades del Estado, así como las empresas públicas, señaladas en la Constitución de la República, de acuerdo con la Disposición General Octava de la Ley, podrán prestar servicios como Entidades de Certificación de Información y Servicios Relacionados, previa resolución emitida por el CONATEL.*
>
> *Las instituciones públicas obtendrán certificados de firma electrónica de las Entidades de Certificación de Información y Servicios Relacionados Acreditadas, de derecho público o de derecho privado."*

En cumplimiento de lo señalado en la Ley de Comercio Electrónico, firmas Electrónicas y Mensajes de Datos, publicada en el suplemento del Registro Oficial No. 577 de fecha 17 de abril de 2002, su Reglamento General y demás normativa aplicable, el Consejo Nacional de Telecomunicaciones CONATEL, a través de la Resolución No. TEL-556-19-CONATEL-2014, de 28 de julio de 2014 resuelve la Acreditación y Registro del Consejo de la Judicatura, como Entidad de Certificación de Información.

1.1 Presentación general del documento

La presente Política de Certificados (PC) de Departamento de Empresa o Institución, se ajusta y complementa las disposiciones contenidas en la Declaración de Prácticas de Certificación (DPC); así como los usos legales, exigencias técnicas y de seguridad requeridos para la emisión y revocación que la entidad de Certificación del Consejo de la Judicatura aplica a este tipo de certificados.

Los Certificados de Departamento de Empresa o Institución, son aquellos que identifican al solicitante como un Departamento de Empresa o Institución y al firmante como representante legal de dicho Departamento de Institución o Empresa, sea esta de derecho público o privado, quien será responsable en tal calidad de todo lo que firme dentro del ámbito de su competencia y límites de uso que correspondan.

1.2 Nombre del documento e identificación

Este documento se denomina Política de Certificados de Departamento de Empresa o Institución, el cual contiene la siguiente información que podrá ser consultada en la página web www.icert.fje.gob.ec en la ubicación http://www.icert.fje.gob.ec/dpc/pc_departamento empresa institucion.pdf

Nombre del documento	***POLITICA DE CERTIFICADOS*** ***Certificados de Departamento de Empresa o Institución***
Descripción	*Los certificados de Departamento de Empresa o Institución acreditan la identidad del suscriptor y le permiten firmar documentos electrónicamente con la misma validez legal que la firma manuscrita.*
Identificador OID	*1.3.6.1.4.1.43745.1.2.3.1*
Versión	*3.0*
Fecha de emisión	*08 de septiembre de 2016*
Ubicación	http://www.icert.fje.gob.ec/dpc/pc_departamento_empresa_institucion.pdf

1.3 Identificación de los tipos de certificado

Cada tipo de certificado recibe su propio OID, indicado e incluido dentro del certificado, en el campo Identificador OID. Cada OID es particular y no se emplea para identificar diferentes tipos, políticas y versiones de los certificados emitidos. El Certificado de Departamento de Empresa o Institución emitido por el Consejo de la Judicatura (CJ) tiene asignado el siguiente identificador de objeto (OID):

1.3.6.1.4.1.43745.1.2.3.1	**Certificado de Departamento de Empresa o Institución**
1.3.6.1.4.1.43745.1.2.3.1.1	Certificado de Departamento de Empresa o Institución - Hardware
1.3.6.1.4.1.43745.1.2.3.1.1.2	Certificado de Departamento de Empresa o Institución - Hardware - HSM SFC
1.3.6.1.4.1.43745.1.2.3.1.2	Certificado de Departamento de Empresa o Institución - Software
1.3.6.1.4.1.43745.1.2.3.1.2.1	Certificado de Departamento de Empresa o Institución - Software - Archivo (PKCS #12)

1.4 Dispositivos para certificados de departamento de empresa o institución

Los dispositivos para certificados de departamento de empresa o institución pueden ser de varios tipos, de conformidad con el contenedor criptográfico:

- Certificados en archivo SW-PKCS #12.
- Certificado en Hardware Dispositivo criptográfico de tipo HW-HSM SFC.

1.5 Administración de la Política de Certificados de Departamento de Empresa o Institución

La Política de Certificados de Departamento de Empresa o Institución es administrada por la Subdirección Nacional de Seguridad de la Información, encargada de su elaboración, actualización, registro y mantenimiento.

Código:	Sustituye a:	Fecha de emisión:	Fecha de revisión:
00-11-A.05-POL3.0-7Política de Certificados de Departamento de Empresa o Institución	00-11-A.05-POL2.0-7Política de Certificados de Departamento de Empresa o Institución	Octubre 2014	Septiembre 2016

A continuación se detallan los datos de la Entidad de Certificación y de una persona de contacto disponibles para responder preguntas respecto a este documento.

1.5.1 Entidad que administra el certificado

ENTIDAD DE CERTIFICACIÓN	*ENTIDAD DE CERTIFICACION ICERT - EC*
NOMBRE	*Subdirección Nacional de Seguridad de la Información*
DIRECCIÓN	*Av. 12 de Octubre N24-593 y Francisco Salazar*
TELÉFONO	*(02) 395 3600*
E-mail	entidad.certificacion@funcionjudicial.gob.ec

1.5.2 Persona de contacto

ENTIDAD DE CERTIFICACIÓN	*ENTIDAD DE CERTIFICACION ICERT - EC*
NOMBRE	*Ing. Reynaldo Gaibor* *Subdirector Nacional de Seguridad de la Información*
DIRECCIÓN	*Av. 12 de Octubre N24-593 y Francisco Salazar*
TELÉFONO	*(02) 395 3600*
E-mail	entidad.certificacion@funcionjudicial.gob.ec

1.5.3 Procedimiento para aprobación de la política

La Política de Certificados de Departamento de Empresa o Institución es administrada por la Subdirección Nacional de Seguridad de la Información y aprobada por el Consejo de la Judicatura.

1.5.4 Publicidad

La Política de Certificados de Departamento de Empresa o Institución es un documento público que se encuentra disponible en la página http://www.icert.fje.gob.ec/dpc/pc_departamento_empresa_institucion.pdf. Las modificaciones a esta política, que fueren aprobadas de acuerdo al procedimiento previsto se publicarán de forma inmediata.

1.6 Entidades y personas participantes

Los certificados de departamento de empresa o institución son emitidos a las personas que acreditan su representación legal del departamento perteneciente a la institución o empresa y documentan su identidad como titulares en la firma de documentos electrónicos, garantizando la legitimidad del emisor de la comunicación y la integridad del contenido. El poseedor de un certificado de departamento de empresa o institución interviene con voluntad en nombre de quien representa e interés propio.

1.6.1 Autoridad de Certificación (AC)

La Autoridad de Certificación es la entidad responsable de emitir y gestionar certificados, garantizar la autenticidad y veracidad de los datos recogidos en el certificado digital expedido, actuar como tercera parte de confianza entre el suscriptor y un usuario de un certificado digital y cuya clave pública está autenticada por el certificado.

La AC además emite los certificados digitales de departamento de empresa o institución de conformidad con los términos establecidos en esta Política de Certificados (PC) y en la Declaración de Prácticas de Certificación (DPC) y garantiza la autenticidad y veracidad de los datos recogidos en el certificado digital expedido.

Las Autoridades de Certificación que componen la PKI del Consejo de la Judicatura son:

AC Raíz: Autoridad de Certificación de primer nivel. Esta AC sólo emite certificados para sí misma y sus AC Subordinadas. Únicamente estará en funcionamiento durante generación del certificado autofirmado; de certificados de AC subordinada y periódicamente para la generación de la lista de certificados revocados de autoridad de certificación raíz ARL o LRA.

AC Subordinada: Autoridad de Certificación subordinada de AC Raíz. Su función es la emisión de certificados de usuario final, de entre otros, Certificados de Departamento de Empresa o Institución.

1.6.2 Autoridad de Registro (AR)

La Autoridad de Registro es la entidad delegada por la Autoridad de Certificación para la identificación y autenticación de los solicitantes de certificados con el fin de receptar y procesar solicitudes de certificados digitales, requiriendo la emisión de los certificados a la AC Subordinada.

Está facultada además para solicitar a la AC Subordinada la revocación, suspensión y reactivación los certificados emitidos por la AC Subordinada.

En la ICERT-EC las Autoridades de Registro son las encargadas de validar la identidad de los solicitantes y mediante procesos certificados y autenticados procesar las solicitudes de certificados.

Los tipos de certificados que emite la ICERT-EC serán para uso de cualquier departamento de empresa o institución interesada.

La Autoridad de Registro llevará un registro completo de los solicitantes que deseen adquirir un certificado.

1.6.3 Solicitante

El solicitante es el representante del departamento de empresa o institución que a nombre de este desea acceder a los servicios de certificación digital para adquirir un certificado de Departamento de Empresa o Institución emitido por la ICERT-EC.

En ningún caso se aceptarán solicitudes de este tipo de certificados a nombre de personas naturales o jurídicas, o terceros que los representan.

1.6.4 Suscriptor

El suscriptor es aquella persona física que demuestra su calidad de representante legal de un departamento de empresa o institución emitido por la ICERT-EC y se considera suscriptor mientras dicho certificado se encuentre vigente.

1.6.5 Terceros que confían

Los terceros que confían son las personas o entidades ajenas al Consejo de la Judicatura que en forma libre y voluntaria deciden confiar en y aceptar un certificado de Departamento de Empresa o Institución emitido por la Autoridad de Certificación.

La ICERT-EC no asume ningún tipo de responsabilidad ante terceros, que, incluso de buena fe, no hayan verificado convenientemente la vigencia de los certificados.

1.7 Ámbito de aplicación de los certificados

1.7.1 Tiempo de validez de los certificados

Los certificados digitales de Departamento de Empresa o Institución tendrán una validez de dos años

1.7.2 Uso apropiado de los certificados

El certificado de Departamento de Empresa o Institución emitido bajo esta política será utilizado solamente durante su período de vigencia, para dar cumplimiento a las funciones que le son propias y legítimas, y puede ser utilizado para los siguientes propósitos:

1.7.2.1 Autenticación de identidad

El certificado puede utilizarse para identificar a un Departamento de Empresa o Institución ante servicios y aplicaciones informáticas, confirmando su autenticidad e integridad.

1.7.2.2 Firma digital

Las firmas digitales efectuadas con Certificados de Departamento de Empresa o Institución ofrecen los medios de respaldo al garantizar la autenticidad del origen, la integridad de los datos firmados y el no repudio.

1.7.2.2.1 Autenticidad del origen

El suscriptor de una comunicación electrónica valida su identidad ante una tercera persona mediante la demostración de la posesión de la clave privada, asociada a la clave pública contenida en el respectivo certificado.

1.7.2.2.2 Integridad del documento

La utilización del certificado garantiza que el documento es integro, es decir, existe la garantía de que el documento no fue alterado o modificado después de firmado por el suscriptor. Además certifica que el mensaje recibido por el usuario es el mismo emitido por el suscriptor.

1.7.2.2.3 No repudio

Evita que el emisor del documento firmado electrónicamente pueda negar en un determinado momento la autoría o la integridad del documento, puesto que la firma del certificado digital puede demostrar la identidad del emisor sin que este pueda repudiarlo.

1.8 Límites de uso de los certificados

Los Certificados de Departamento de Empresa o Institución emitidos por la ICERT-EC no pueden ser utilizados para actuar ni como Autoridad de Registro ni como Autoridad de Certificación, firmando otros certificados de clave pública de ningún tipo, ni listas de certificados revocados (CRL). Tampoco pueden ser usados para fines contrarios a la legislación vigente.

1.9 Usos prohibidos de los certificados

La realización de operaciones no autorizadas según esta Política de Certificados, por parte de terceros o suscriptores del servicio, eximirá a la ICERT-EC de cualquier responsabilidad por este uso prohibido, en consecuencia:

- No se permite el uso del certificado de Departamento de Empresa o Institución para firmar otros certificados o listas de revocación (CRL)
- Está prohibido utilizar el certificado para usos distintos a los estipulados en los numerales correspondientes a: ***Usos apropiados de los certificados*** y ***Límites de uso de los certificados*** de la presente Política de Certificados.
- No están permitidas alteraciones sobre los certificados emitidos por la ICERT-EC.
- No está permitido el uso de certificados que puedan ocasionar daños personales o medioambientales.
- Se prohibe toda acción que infrinja las disposiciones, obligaciones y requisitos estipulados en la presente Política de Certificados.
- No está permitido emitir valoración alguna sobre el contenido de los documentos que firma el suscriptor, debido a que el contenido del mensaje es de su exclusiva responsabilidad.
- No está autorizado por parte de la ICERT-EC, recuperar los datos cifrados en caso de pérdida de la clave privada del suscriptor porque la CA por seguridad no guarda copia de la clave privada de los suscriptores, por lo tanto es responsabilidad del suscriptor la utilización de sus datos.

1.10 Exención de responsabilidad

La ICERT-EC quedará exenta de responsabilidad por daños y perjuicios cuando el usuario exceda los límites de uso indicados para este tipo de certificados.

La Entidad de Certificación Consejo de la Judicatura deslinda toda responsabilidad concerniente a solicitudes de certificados y registros de suscriptores realizados con suplantación de identidad o datos fraudulentos.

1.11 Definiciones

En el desarrollo de la presente DPC los términos empleados y sus correspondientes definiciones son los siguientes:

Auditoría: Procedimiento utilizado para comprobar la eficiencia de los controles establecidos a la operación de la entidad, en la prevención y detección de fraudes o mediante la realización de exámenes a aplicaciones concretas, que garanticen la fiabilidad e integridad de sus actividades.

Autenticación: Proceso electrónico mediante el cual se verifica la identidad de un usuario, solicitante o suscriptor de un certificado emitido por la ICERT-EC.

Autoridad de Certificación (AC): Entidad encargada de emitir y revocar certificados digitales utilizados en firma electrónica y cuya clave pública está incluida en el.

Autoridad de Registro (AR): Entidad encargada de receptar las solicitudes de certificados, identificar y autenticar la información de los solicitantes de certificados, aprobar o rechazar las solicitudes de certificados, revocar o suspender certificados o en determinadas circunstancias, y aprobar o rechazar las solicitudes para renovar o volver a introducir su certificados.

ARL (Authority Revocation List): Lista de certificados revocados emitida por la AC Subordinada que contiene la lista de todos los certificados de AC Subordinada emitidos por la AC Raíz que hayan sido revocados o suspendidos y que aún no hayan expirado.

CRL (Certificate Revocation List): Lista de certificados que han sido revocados.

Clave privada: En un criptosistema de claves públicas es la clave, de un par de claves de un usuario, que es conocida solamente por el usuario o titular del certificado.

Clave pública: En un criptosistema de claves públicas es la clave, de un par de claves de un usuario, que se conoce públicamente. La clave pública pertenece a la AC, se incluye en el certificado digital.

Cadena de confianza: También conocida como Jerarquía de Confianza, la constituyen las autoridades de certificación relacionadas por la confiabilidad en la emisión de certificados digitales entre diferentes niveles jerárquicos. En el caso del CJ existen la Autoridad de Certificación Raíz y la Autoridad de Certificación Subordinada.

Datos personales: Son aquellos datos o información de carácter personal o íntimo, que son materia de protección en virtud de la Ley 2002 - 67.

Datos personales autorizados: Son aquellos datos personales que el titular ha accedido a entregar o proporcionar de forma voluntaria, para ser usados por la persona, organismo o entidad de registro que los solicita, solamente para el fin para el cual fueron recolectados, hecho que debe constar expresamente señalado y ser aceptado por dicho titular.

Desmaterialización de documentos: Los documentos desmaterializados se considerarán, para todos los efectos, copia idéntica del documento físico a partir del cual se generaron y deberán contener adicionalmente la indicación de que son desmaterializados o copia electrónica de un documento físico. Se emplearán y tendrán los mismos efectos que las copias impresas certificadas por autoridad competente. Los documentos desmaterializados deberán señalar que se trata de la desmaterialización del documento original. Este señalamiento se constituye en la única diferencia que el documento desmaterializado tendrá con el documento original. (Art. 4 y 5 del Reglamento a la Ley de Comercio Electrónico).

HSM (Hardware Security Module): Es un componente o dispositivo criptográfico utilizado para generar, almacenar y proteger claves criptográficas.

OCSP (Online Certificate Status Protocol): Protocolo informático utilizado para comprobar el estado de un certificado digital en el momento en que es utilizado. Proporciona información actualizada y complementaria del listado de certificados revocados.

OID (Object Identifier): El Identificador de Objetos constituye el valor de una secuencia de componentes variables utilizado para nombrar a casi cualquier tipo de objeto en los certificados digitales, tales como los componentes de los nombres distinguidos, DPC, etc.

PKCS (Public Key Cryptography Standard): Estándares de criptografía de claves públicas.

PKCS #10: Estándar de criptografía de clave pública utilizado para procesar la petición de un certificado y solicitar la generación de una clave.

PKCS #12: Estándar de criptografía de clave pública que define un formato de fichero utilizado para almacenar claves privadas con su certificado de clave pública protegido mediante clave simétrica.

PKI (Public Key Infrastructure): Infraestructura de Clave Pública es el conjunto de elementos informáticos (hardware y software), políticas y procedimientos necesarios para brindar servicios de certificación digital.

Política de Certificados: Documento que complementa la Declaración de Prácticas de Certificación y que contiene un conjunto de reglas que norman las condiciones de uso y los procedimientos seguidos por la ICERT-EC para la emisión de certificados, determinando la aplicabilidad de un certificado a un grupo o comunidad en particular y/o a una clase de aplicaciones con requisitos comunes de seguridad.

RFC (Request for comments): Publicaciones de *Internet Engineering Task Force* que en forma de memorandos contienen protocolos y procedimientos para regular el funcionamiento de Internet.

Sellado de tiempo: Anotación firmada electrónicamente y agregada a un mensaje de datos mediante procedimientos criptográficos en la que consta como mínimo la fecha, la hora y la identidad de la persona que efectúa la anotación, basándose en el RFC 3161 Internet X.*509 Public Key Infrastructure Time-Stamp Protocol (TSP)*.

X.509: Estándar desarrollado por la UIT-T para infraestructuras de clave pública que especifica entre otros temas, los formatos estándar para certificados de clave pública y para la implementación de listas de certificados revocados.

1.12 Siglas

AC: **A**utoridad de **C**ertificación
AR: **A**utoridad de **R**egistro
ARL **A**uthority **R**evocation **L**ist
AV: **A**utoridad de **V**alidación
C **C**ountryName
CA **C**ertification **A**uthority (Autoridad de Certificación AC)

CJ	**C**onsejo de la **J**udicatura
CN	**C**ommon**N**ame
cps	**c**ertificate **p**ractice **s**tatement
CRL	**C**ertificate **R**evocation **L**ist (Lista de certificados revocados)
DN	**D**istinguished **N**ame
DPC	**D**eclaración de **P**rácticas de **C**ertificación
DNTICs	**D**irección **N**acional de **T**ecnologías de la **I**nformación y **C**omunicaciones
ERC	**E**mergency **R**evocation **C**ode
HSM	**H**ardware **S**ecurity **M**odule (Módulo de Seguridad Criptográfica)
HTTP	**H**ypertext **T**ransfer **P**rotocol
HTTPS	**HTTP S**ecure
ICERT-EC	Entidad de Certificación del Consejo de la Judicatura
IP	**I**nternet **P**rotocol
ISO	**I**nternational **O**rganization for **S**tandardization
L	**L**ocalityName
NIST	**N**ational **I**nstitute of **S**tandards and **T**echnology
O	**O**rganizationName
OCSP	**O**nline **C**ertificate **S**tatus **P**rotocol (Protocolo de estatus de certificados en línea)
OID	**O**bject **Id**entifier (Identificador de Objetos)
OU	**O**rganizational**U**nitName
PC	**P**olítica de **C**ertificados
PDF	**P**ortable **D**ocument **F**ormat
PDF/A	**PDF/A**rchive
PIN	**P**ersonal **I**dentification **N**umber
PKCS	**P**ublic-**K**ey **C**ryptography **S**tandard (Estándares de criptografía de clave pública)
PKI	**P**ublic **K**ey **I**nfrastructure (Infraestructura de Clave Pública)
PUK	**P**ersonal **U**nlok **K**ey (Clave personal de desbloqueo)
RA	**R**egistration **A**uthority (Autoridad de Registro AR)
RFC	**R**equest **F**or **C**omments (Petición de comentarios)
RSA	**R**ivest **S**hamir **A**dleman
RUC	**R**egistro **Ú**nico de **C**ontribuyentes
SFC	**S**ervidor de **F**irma **C**entralizada
SHA	**S**ecure **H**ash **A**lgorithm
SW	**S**oft**w**are
TSP	**T**ime-**S**tamp **P**rotocol
URL	**U**niform **R**esource **L**ocator
UTC	**U**niversal **T**ime **C**oordinated
UTF-8	**8**-bit **U**nicode **T**ransformation **F**ormat
v	**v**ersion

VA **V**alidation **A**uthority (Autoridad de Validación AV)

1.13 Referencias a otros documentos

[RFC5280] RFC 5280. Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile. May 2008.

[LEY2002-67] Ley No. 2002-67. Ley de comercio electrónico, firmas electrónicas y mensajes de datos. Dada en la ciudad de San Francisco de Quito, Distrito Metropolitano, en la sala de sesiones del Pleno del Congreso Nacional del Ecuador, a 10 de abril del 2002.

[DECRETO-3496] Decreto No. 3496. Reglamento a la Ley de comercio electrónico, firmas electrónicas y mensajes de datos. Dado en el Palacio Nacional, en Quito, a 12 de diciembre del 2002.

[DECRETO-1356] Decreto Nº 1356. Reformas al Reglamento general a la Ley de comercio electrónico, firmas electrónicas y mensajes de datos. Dado en el Palacio Nacional, en San Francisco de Quito, el día de 29 de septiembre de 2008.

[DECRETO-867] Decreto Nº 867. Reforma al Reglamento general a la Ley de comercio electrónico, firmas electrónicas y mensajes de datos. Registro Oficial Nº 532. Quito, Lunes 12 de Septiembre del 2011.

[MINTEL-181] Ministerio de Telecomunicaciones y de la Sociedad de la Información. Acuerdo Nº 181. Dado en Quito, Distrito Metropolitano, a 15 de septiembre de 2011.

[MINTEL-012] Ministerio de Telecomunicaciones y de la Sociedad de la Información. Acuerdo Nº 012-2016. Dado en Quito, Distrito Metropolitano, a 23 de mayo de 2016.

Código:	Sustituye a:	Fecha de emisión:	Fecha de revisión:
00-11-A.05-POL3.0-7Política de Certificados de Departamento de Empresa o Institución	00-11-A.05-POL2.0-7Política de Certificados de Departamento de Empresa o Institución	Octubre 2014	Septiembre 2016

2. PUBLICACIÓN Y REGISTRO DE CERTIFICADOS

Las políticas de certificados de la ICERT-EC, la información del directorio de certificados, los medios de publicación, la frecuencia de publicación y el control de acceso al directorio de certificados estarán disponibles para suscriptores de acuerdo a las políticas que establezca la Entidad de Certificación de Información ICERT-EC.

Cualquier cambio o modificación en la Política de Certificados de Departamento de Empresa o Institución generará una nueva versión, debiendo publicarse dicho cambio, además de guardar y custodiar la versión anterior, toda vez que al amparo de esta última pudiesen haberse originado derechos y obligaciones para los suscriptores y usuarios.

Es responsabilidad de la Entidad de Certificación la adopción de las medidas de seguridad necesarias para garantizar la integridad, autenticidad y disponibilidad de dicha información.

3. IDENTIFICACIÓN Y AUTENTICACIÓN

En esta sección se describen los procedimientos específicos y criterios aplicados por las Autoridades de Registro y la Autoridad de Certificación de la ICERT-EC en el momento de autenticar la identidad del solicitante y aprobar la emisión de un certificado de Departamento de Empresa o Institución.

3.1 Registro inicial

Previo a la emisión inicial de un certificado de departamento de empresa o institución, el solicitante deberá realizar el ingreso de datos del usuario necesarios para la emisión del certificado a través de un formulario de registro en Internet.

La Autoridad de Registro de la ICERT-EC realizará el procedimiento necesario para identificar y validar la información del solicitante de un certificado, con el fin de brindar confianza equivalente para cualquier suscriptor de un certificado emitido por la AC.

3.2 Nombres

De acuerdo a la presente Política de Certificados se establece la necesidad de la plena identificación del suscriptor y la asignación de un nombre significativo a su certificado, para vincular la clave pública con su identidad.

3.2.1 Tipos de nombres

Todos los certificados de departamento de empresa o institución tienen una sección llamada Subject cuyo objetivo es permitir identificar al suscriptor o titular del certificado, incluyendo un Distinguished Name (DN) caracterizado por un conjunto de atributos que conforman un nombre diferenciado, único e inequívoco para cada suscriptor de los certificados emitidos por la ICERT-EC.

Abrev.	Nombre	Descripción
C	País	*Abreviatura del país donde reside el suscriptor*
L	Ciudad	*Abreviatura de la ciudad donde reside el suscriptor*
SerialNumber	Número Serial	*Número del documento identificación del representante legal*
CN	Nombre común	*Nombres y apellidos completos del suscriptor*

3.2.2 Necesidad de que los nombres sean significativos

Todo certificado de Departamento de Empresa o Institución emitido por la ICERT-EC tiene como característica principal la plena identificación del suscriptor y la asignación de un nombre significativo a su certificado, para vincular la clave pública con su identidad.

3.2.3 Anónimos y pseudónimos en los nombres

De acuerdo a esta Política de Certificados no se admiten anónimos ni seudónimos para identificar el nombre de un Departamento de Empresa o Institución.

En el caso de un Departamento de Empresa o Institución domiciliada en el Ecuador, el nombre o razón social debe estar de acuerdo a como cómo consta en el Acta Constitutiva de la Empresa o Institución Matriz. Si la Empresa o Institución es extranjera, el nombre o razón social del Departamento de Empresa o Institución debe estar conformado por nombres tal como consta en el Acta de Constitución o documento equivalente de la Empresa o Institución Matriz.

3.2.4 Reglas para la interpretación de diversas formas de nombre

Las reglas para interpretar los formatos de nombre siguen lo señalado por el estándar X.500 de referencia en ISO/IEC 9594.

Todos los nombres de departamentos de empresa o institución están escritos utilizando lenguaje natural, prescindiendo de acentos. En ningún caso se pueden modificar los nombres de un Departamento de Empresa o Institución, ni de su representante legal excepto para adaptarlos al formato y longitud del componente Common Name en el que se insertan.

3.2.5 Unicidad de los nombres

Los nombres distintivos en los certificados de departamento de empresa o institución están relacionados con el identificador de usuario y son únicos para cada suscriptor porque contienen caracteres de serie que permiten distinguir entre dos identidades cuando existan problemas de homónimos de nombres.

3.3 Validación inicial de la identidad

3.3.1 Método para probar la posesión de la clave privada

La clave privada del certificado de departamento de empresa o institución es generada aleatoriamente. Para demostrar que el titular posee la clave privada correspondiente a la clave pública que se pretende vincular al certificado de departamento de empresa o institución, se probará mediante el envío de la petición de certificado, en la cual se incluirá la clave pública mediante la clave privada asociada.

Los modos de generación de claves en la ICERT-EC son los siguientes:

a) Generación y construcción de un PKCS#12 descargable

La AR permite realizar al operador de emisión la generación de un par de claves de firma y del certificado emitido por la AC, y permite el envío por correo electrónico del par de claves y del certificado en formato de archivo PKCS#12.

b) Generación en HSM SFC y custodia segura remota

La RA permite realizar al operador de emisión la generación del par de claves de firma en un HSM y del certificado emitido por la AC, y procederá al almacenamiento seguro de las claves. Estas claves cifradas serán solamente utilizables por el suscriptor a través de un software seguro destinado a este propósito y a través del SFC.

Una vez finalizado el proceso, la AR envía al suscriptor las credenciales de acceso a su clave privada por correo electrónico. Las credenciales establecidas son calculadas a través de algoritmos y completamente desconocidas para terceras partes.

La clave privada es accesible sólo a través de medios que conoce exclusivamente el suscriptor y permanece bajo su custodia.

3.3.2 Autenticación de la identidad de Departamento de Empresa o Institución

El solicitante para demostrar su identidad debe proporcionar la siguiente información y documentación para adquirir el certificado de departamento de empresa o institución, conforme a la normativa aplicable y al cuadro de identificadores de campo:

NUMERO IDENTIFICADOR	CAMPOS
3.10	***Razón Social***
3.11	***RUC***
3.1	***Cédula o Pasaporte del suscriptor***
3.2	***Nombres del suscriptor***
3.3	***Primer apellido del suscriptor***
3.4	***Segundo apellido del suscriptor***
3.5	***Cargo***
3.7	***Dirección***
3.8	***Teléfono***
3.9	***Ciudad***
3.12	***País***

La información suministrada por el solicitante a través de la página web a la Autoridad de Registro, será revisada por el operador de validación quien es el encargado de verificar que la información sea auténtica, suficiente y adecuada de acuerdo a los procedimientos internos definidos por la ICERT-EC.

3.3.3 Información de solicitante no verificada

En la solicitud del certificado de departamento de empresa o institución el solicitante debe proporcionar documentos y datos personales que lo identifican absolutamente, toda la información solicitada será verificada aún si no hace parte de la información incluida en el certificado digital. Se debe dejar constancia de la información no verificada.

3.3.4 Identificación y autenticación para solicitudes de revocación

El procedimiento para identificación y autenticación para generar la solicitud de revocación de un certificado requiere de la autenticación del suscriptor con sus credenciales, que consisten en el identificador unívoco de la solicitud y en el código de emergencia asociado ERC.También puede ser procesada mediante una solicitud enviada por un tercero debidamente identificado que represente al suscriptor. Asimismo, también es posible mediante una comparecencia física, por la que el operador de validación procederá a la revocación.

4. REQUISITOS OPERACIONALES PARA EL CICLO DE VIDA DE LOS CERTIFICADOS

Los certificados de departamento de empresa o institución emitidos por la ICERT-EC tienen un período de validez puesto de manifiesto en el propio certificado. En el contrato correspondiente se indica además, el tiempo de vigencia de dicho certificado.

4.1 Solicitud de certificados

4.1.1 Persona apta para presentar una solicitud de certificado

La solicitud de un certificado de departamento de empresa o institución la puede realizar el representante legal o su delegado debidamente acreditado, y que esté en plena capacidad legal para contratar y obligarse de cumplir con las responsabilidades inherentes al uso de dicho certificado.

4.1.2 Presentación de solicitud de certificado

Todo departamento de empresa o institución que desee obtener un certificado de firma electrónica emitido por la ICERT-EC, debe realizar la solicitud de certificado a través de la página web a la Autoridad de Registro de la ICERT-EC.

4.1.3 Comprobación de solicitudes

El operador de validación deberá comprobar y validar la información y los documentos que son requeridos para solicitar los certificados de departamento de empresa o institución.

Para estos efectos el solicitante autoriza y faculta expresamente a la ICERT-EC que verifique los la información proporcionada con otras bases de datos públicas o privadas.

La Autoridad de Registro de la ICERT-EC mantendrá un archivo con la información que respalde cada solicitud de inscripción realizada para la emisión de los certificados de departamento de empresa o institución, por un período mínimo de cinco (5) años.

4.1.4 Procedimiento de solicitud de certificados y responsabilidades de los solicitantes

El procedimiento que debe realizar el solicitante para la emisión de un certificado de departamento de empresa o institución es el siguiente:

No.	Responsable	Descripción de la actividad	Documentos de apoyo
1	Usuario suscriptor	Ingresa solicitud a través de la web	Documentos escaneados
2	Operador de validación	Revisa solicitudes, aprueba o archiva las solicitudes (Si fue aprobada se notifica al usuario el valor a pagar por tipo de certificado)	Documentos escaneados
3	Operador de validación	A través del sistema se archiva las solicitudes aprobadas de las que no se ha emitido el certificado en más de 30 días	

Es responsabilidad del solicitante garantizar la veracidad de toda la información proporcionada para obtener su certificado de departamento de empresa o institución. La ICERT-EC verificará que los datos proporcionados por el solicitante sean fidedignos.

4.1.5 Aprobación de la solicitud

Si el proceso de verificación y validación de la documentación e información entregada por el solicitante resulta exitosa, la Autoridad de Registro de la ICERT-EC aceptará la solicitud de emisión de certificado.

4.1.6 Archivo de la solicitud

Se archivarán notificando la causa, las solicitudes que no cumplan con los requerimientos, información y documentación solicitados en la presente Política de Certificados de Departamento de Empresa o Institución, o que los documentos presentados no sean concordantes. El archivo de la solicitud rechazada da lugar a que el solicitante pueda nuevamente iniciar el proceso de solicitud de certificado, esto se aplicará también para solicitudes que hayan sido aprobadas y que no se ha realizado el registro de pago en los treinta días posteriores a su aprobación.

4.1.7 Registro de pago

El usuario cuya solicitud ha sido aprobada presentará ante el operador de emisión su comprobante de pago, el que se ingresará en el sistema junto con la factura correspondiente. Una vez realizado el pago el usuario tiene un tiempo de treinta (30) días para acercarse para la emisión del certificado. De no presentarse en el tiempo establecido se archivará la solicitud y el valor pagado no será reembolsable.

4.2 Emisión de certificados

Una vez aprobada la solicitud de certificado y realizado el pago correspondiente, el operador de emisión de la Autoridad de Certificación de la ICERT-EC emitirá el certificado a nombre del suscriptor, siendo el mismo personal e intransferible.

La generación de un certificado de usuario se realizará desde la interfaz web de administración y operación, por un operador de la Entidad de Certificación con un rol dinámico con permisos para emitir certificados.

El procedimiento para la emisión de certificados digitales que se describe en la presente Política de Certificados está soportado por el Sistema PKI de la ICERT-EC y contempla los siguientes pasos:

No.	Responsable	Descripción de la actividad	Documentos de apoyo
1	Operador de emisión	Revisa que no haya caducado el pago para el certificado a emitir	
2	Operador de emisión	Valida la información que se ingresó mediante solicitud	Documentos escaneados
3	Usuario Suscriptor	Entrega documentos de identidad y presenta comprobante de pago y factura	Comprobante de pago y factura

Código:	Sustituye a:	Fecha de emisión:	Fecha de revisión:
00-11-A.05-POL3.0-7Política de Certificados de Departamento de Empresa o Institución	00-11-A.05-POL2.0-7Política de Certificados de Departamento de Empresa o Institución	Octubre 2014	Septiembre 2016

No.	Responsable	Descripción de la actividad	Documentos de apoyo
4	Operador de emisión	Genera el certificado de acuerdo a contenedor solicitado, toma fotografía y genera el contrato. Se envía el sobre de credenciales al usuario	Contrato, correo electrónico con códigos
5	Usuario Suscriptor	El usuario firma el contrato	Contrato firmado
6	Operador de emisión	Almacena el contrato y lo envía vía correo	Contrato firmado

4.2.1 Acciones de la AC durante la emisión del certificado

Con la emisión del certificado por parte de la AC de la ICERT-EC se perfecciona la aprobación definitiva de la solicitud realizada por parte del representante del Departamento de Empresa o Institución.

Todos los certificados entrarán en vigencia desde el momento de su emisión. El periodo de vigencia estará sujeto a una posible extinción anticipada, temporal o definitiva, cuando se den las causas que motiven la suspensión o revocación del certificado.

4.2.2 Notificación al suscriptor por parte de la AC de la emisión del certificado

La notificación al suscriptor respecto de la emisión del certificado se realizará a través del correo electrónico provisto por éste durante la inscripción de sus datos, previa a la emisión del certificado.

4.3 Aceptación del certificado

4.3.1 Aceptación del certificado por el solicitante

La aceptación del certificado digital se da el momento en que el titular del certificado expresa la aceptación de los términos y condiciones contenidos en el contrato de prestación de de los servicios de certificación de información y servicios relacionados que suscribe con la ICERT-EC.

Si la AC no recibe ninguna notificación por parte del suscriptor dentro de las cuarenta y ocho (48) horas posteriores a la emisión del certificado se considerará la aceptación de éste. Un suscriptor puede enviar un mensaje de no aceptación del certificado incluyendo el motivo del rechazo y la identificación de los motivos, o de ser el caso los campos en el certificado que están incorrectos o incompletos.

4.3.2 Publicación del certificado por la AC

Emitido el certificado de Departamento de Empresa o Institución por parte de la ICERT-EC, se procede a la publicación en el directorio de certificados. La clave pública del certificado es publicada en el correspondiente repositorio de Base de Datos de la AR.

4.4 Par de claves y uso del certificado

4.4.1 Uso de la clave privada y del certificado por parte del suscriptor

El suscriptor posee una clave pública y una clave privada legalmente válidas durante el periodo de vigencia del certificado de departamento de empresa o institución. La clave privada es de uso exclusivo del suscriptor para los fines estipulados en esta Política de

Certificados.

El suscriptor sólo podrá utilizar la clave privada y el certificado exclusivamente para los usos autorizados en esta Política de Certificados. De igual manera, el suscriptor solo podrá utilizar el par de claves y el certificado tras aceptar las condiciones de uso, establecidas en la DPC y ésta PC, y sólo para la realización de funciones que requieran acreditar la identidad del titular como Departamento de Empresa o Institución.

Una vez que el certificado haya expirado o este revocado el suscriptor dejará de usar la clave privada.

4.4.2 Uso de la clave pública y del certificado por los terceros que confían

Los terceros que confían en los servicios de certificación de la ICERT-EC solo pueden depositar su confianza en los certificados de funciones que requieran acreditar la identidad del titular como Departamento de Empresa o Institución, de conformidad con lo establecidos en el campo "keyUsage" del certificado o en la presente Política de Certificados.

Los usuarios que confían en el servicio de certificación de la ICERT-EC deben verificar el estado del certificado utilizando los mecanismos establecidos en la DPC y en la presente PC.

4.5 Renovación de certificados

La renovación del certificado se produce cuando éste va a expirar y el suscriptor desea continuar usando un certificado. Para esto el suscriptor deberá realizar el mismo procedimiento utilizado para solicitar un certificado. De haberse producido cambios en los datos que constan en el primer certificado será necesario acompañar la documentación requerida para el registro de esta información dentro del certificado.

Sin perjuicio de lo señalado en el inciso anterior, la Autoridad de Registro de la ICERT-EC, notificará al suscriptor con la antelación necesaria, la expiración del certificado a través de un correo electrónico a la dirección de e-mail registrada por el suscriptor.

4.5.1 Razones para la renovación de certificados

La Autoridad de Registro de la ICERT-EC, notificará al suscriptor con anticipación a la fecha de expiración del certificado a través de un correo electrónico a la dirección de e-mail registrada.

Esta notificación se hace en beneficio del suscriptor para facilitarle el proceso de renovación antes indicado.

En todas las renovaciones de certificados realizadas en el ámbito de esta Política de Certificados se generarán un nuevo par de claves.

4.6 Renovación de certificados con cambio de claves

Todas las renovaciones de certificados de Departamento de Empresa o Institución, independientemente de su causa, se realizarán siempre con cambio de claves. Este proceso de renovación seguirá el mismo procedimiento empleado para la emisión inicial de los certificados.

4.6.1 Circunstancias para la renovación de un certificado con cambio claves

Circunstancias por las que se puede renovar un certificado:

- Está en el período de renovación configurado en la política de certificación o se ha producido la expiración del periodo de validez.
- No está revocado.

4.6.2 ¿Quién puede solicitar la renovación de los certificados?

La renovación de los Certificados de Departamento de Empresa o Institución, únicamente puede ser solicitada por sus titulares, previo a su expiración.

4.6.3 Procesamiento de las solicitudes de renovación de certificados

Una solicitud de renovación de certificado se procesa de igual manera que la solicitud inicial de un certificado.

Las renovaciones de Certificados de Departamento de Empresa o Institución, están sujetas a las siguientes condiciones:

- Que se requiera, previa su expiración.
- Que la solicitud de renovación se refiera al mismo tipo de certificado emitido inicialmente.

4.6.4 Conducta de aceptación del certificado renovado

Se establecen las mismas condiciones de aceptación que se determinan en la emisión inicial de Certificados de Departamento de Empresa o Institución.

4.7 Modificación de certificados

4.7.1 Circunstancias para la modificación de un certificado

Aunque se produjesen cambios relacionados con el nombre, cargo o funciones desempeñadas por un suscriptor, el certificado no puede ser modificado. Todas las modificaciones de certificados realizadas en el ámbito de esta PC se tratarán como una nueva emisión de certificado.

Se modifica un certificado cuando se revoca y se emite uno nuevo, por motivos de cambios de datos o información del certificado no relacionada con su clave pública.

Las modificaciones pueden darse si se desea modificar alguno de los datos del usuario, con respecto a sus anteriores certificados, antes de la emisión de un nuevo certificado del usuario.

4.8 Revocación y suspensión y reactivación de certificados

La revocación y suspensión de los certificados son mecanismos que se utilizan cuando existe la pérdida de fiabilidad de los mismos, ocasionando el cese de su operatividad e impidiendo su uso legítimo.

La revocación, suspensión y reactivación de un certificado desde la AR puede ser realizada por un operador de la AR o por el usuario que solicitó el certificado.

En la Declaración de Prácticas de Certificación de la ICERT-EC se especifican las razones por las cuales se puede revocar o suspender un certificado digital, los medios para efectuarlas, el procedimiento, y el tiempo que se tarda en procesar y resolver la suspensión o revocación.

La revocación de un certificado tiene como principal efecto la terminación inmediata y anticipada del periodo de validez del mismo. Este acto no afectará las obligaciones subyacentes creadas o comunicadas por esta PC ni tendrá efectos retroactivos.

Los certificados revocados no podrán bajo ninguna circunstancia volver al estado activo.

La revocación de un certificado implica su publicación en la Lista de Certificados Revocados (CRL) de acceso público.

Los certificados suspendidos podrán volver al estado activo.

La suspensión de un certificado implica su publicación en la Lista de Certificados Revocados (CRL) hasta que este sea reactivado, de no ser este el caso este permanecerá definitivamente en la Lista de Certificados Revocados (CRL).

4.8.1 Circunstancias para la revocación

Los certificados emitidos por la Autoridad de Certificación de la ICERT-EC pueden ser revocados por los siguientes motivos:

- Traslado de funciones.
- Cesación de funciones.
- Por robo, sustracción, pérdida, modificación o revelación de la clave que permite la activación de la clave privada del titular.
- Cambio de datos en el certificado.
- El mal uso de claves y certificados, o la falta de observancia o contravención de los requerimientos operacionales.
- La emisión defectuosa de un certificado debido a que:
  - No se ha cumplido con algún requisito para la emisión del certificado.
  - Uno o más datos fundamentales relativos al certificado son falsos.
  - Existe error en el ingreso de datos u otro error en el proceso.
- El certificado de una AR o AC superior en la jerarquía de confianza del certificado es revocado.
- Fallecimiento del titular del certificado.
- Por el cese en la actividad como prestador de servicios de certificación por parte del ICERT-EC.

4.8.2 Circunstancias para la suspensión

La suspensión de un certificado implica su invalidez durante el período en que permanece suspendido.

Las circunstancias para la suspensión de un certificado son:

- Pérdida temporal del contenedor, que no involucre que las claves estén comprometidas.
- Por pedido del suscriptor.

4.8.3 Procedimiento para la solicitud de suspensión

La suspensión de un certificado únicamente opera cuando la ICERT-EC recibe una solicitud debidamente fundamentada por parte del suscriptor la que debe ser dirigida a la AR, o cuando se sospecha que la clave privada ha sido comprometida. En el caso de una empresa o institución se puede solicitar la suspensión mediante una carta.

4.8.4 Plazo límite del tiempo de suspensión

El plazo máximo que puede permanecer suspendido es un periodo igual al tiempo que resta para la caducidad del certificado.

4.9 Servicios de información del estado del certificado

La ICERT-EC proporciona el servicio de información del estatus de los certificados a través de las CRL publicadas en su página web o través de la Autoridad de Validación AV mediante el protocolo OCSP.

4.10 Finalización de la suscripción

En el certificado de Departamento de Empresa o Institución se especifica el tiempo de su validez plena y legal, ya que se determina desde y hasta cuando está vigente.

Código:	Sustituye a:	Fecha de emisión:	Fecha de revisión:
00-11-A.05-POL3.0-7Política de Certificados de Departamento de Empresa o Institución	00-11-A.05-POL2.0-7Política de Certificados de Departamento de Empresa o Institución	Octubre 2014	Septiembre 2016

5. CONTROLES DE SEGURIDAD FÍSICA, INSTALACIONES, GESTIÓN Y OPERACIONALES

Los aspectos referentes a los controles de seguridad: física, de las instalaciones, de personal, auditoría y operacionales definidos para trabajar en un ambiente fiable y seguro, se encuentran especificados en la Declaración de Prácticas de Certificación de la ICERT-EC.

6. CONTROLES DE SEGURIDAD TÉCNICA

La Infraestructura de Clave Pública PKI del Consejo de la Judicatura utiliza sistemas y productos fiables, que cumplen las normas y certificaciones internacionales sobre la materia, se encuentran protegidos contra toda alteración y de esta manera garantizan la seguridad técnica y criptográfica de los procesos de certificación.

6.1 Generación e instalación del par de claves

6.1.1 Generación del par de claves

El par de claves para los componentes internos de la Infraestructura de Clave Pública del Consejo de la Judicatura, se generan en módulos de hardware criptográficos que cumplen los requisitos establecidos en un perfil de protección de dispositivo seguro de firma electrónica y de Autoridad de Certificación normalizado.

La generación del par de claves del suscriptor varía de acuerdo a la forma de entrega del certificado elegido por el suscriptor o de acuerdo al convenio:

- Entrega del par de claves y certificado en archivo con formato PKCS #12.
- Se entregan las credenciales para el acceso al par de claves y certificado almacenados remotamente y generados en un HSM (SFC) a través de la librería PKCS#11. El par de claves para los certificados se generan en dispositivos criptográficos hardware con certificación FIPS 140-2 Nivel 3 y/o Common Criteria EAL4+ (CWA14169).

6.1.2 Entrega de la clave privada al suscriptor

Para el certificado en archivo formato PKCS#12 la clave privada se encuentra contenida en el archivo y se enviará en por e-mail al suscriptor. En un e-mail adicional se enviará la contraseña del archivo PKCS#12.

En el caso de certificados en HSM SFC, la clave es generada y cifrada en el HSM por el operador de AR bajo la presencia del suscriptor, posteriormente es almacenada en el SFC y su uso es protegido mediante el uso de credenciales que sólo el suscriptor tiene conocimiento.

6.1.3 Entrega de la clave pública al suscriptor

El mecanismo de entrega de la clave pública a titulares de certificados de departamento de empresa o institución varía si la forma de entrega es en archivo con formato PKCS#12 o en HSM SFC.

La clave pública de los certificados de departamento de empresa o institución se genera en el puesto de emisión siendo la AR la responsable de entregar dicha clave pública a la AC.

6.1.4 Disponibilidad de la clave pública

La clave pública de los usuarios está disponible a través de la base de datos y tendrán acceso los usuarios suscriptores a través de la AR.

6.1.5 Periodo de utilización de la clave privada

El periodo de utilización de la clave privada es el mismo tiempo de la vigencia del certificado

de departamento de empresa o institución o inferior cuando el certificado es revocado antes de caducar.

6.1.6 Tamaño de las claves

El tamaño de las claves de certificados de departamento de empresa o institución es de 2048 bits.

6.1.7 Parámetros de generación de la clave pública y verificación de la calidad

La clave pública de la AC Raíz y de la AC Subordinada está codificada de acuerdo con RFC 5280. El algoritmo de generación de claves es sha256withRSAEncryption.

La clave pública de los certificados emitidos por la PKI del CJ está codificada de acuerdo con RFC 5280. El algoritmo de generación de claves es sha256withRSAEncryption.

6.1.8 Fines de uso de la clave X.509 v3

Todos los certificados de departamento de empresa o institución emitidos a través de la infraestructura de Clave Pública del Consejo de la Judicatura contienen la extensión 'keyUsage' definida por el estándar X.509 v3, la cual se califica como crítica.

6.2 Controles sobre la clave privada del suscriptor

En el cuadro siguiente se especifican los controles de protección de la clave privada del suscriptor según la forma de entrega del certificado; no obstante, la protección de los datos de activación es responsabilidad exclusiva del suscriptor.

Control de la ICERT-EC para protección de la clave privada	Forma de entrega del certificado	
	Archivo PKCS #12	**HSM SFC**
Respaldo de la clave privada	ICERT-EC no realiza respaldo de los archivos PKCS#12 ni de la clave privada en él contenida. Una vez generado es enviado al suscriptor.	ICERT-EC no realiza respaldo legible o que pueda utilizarse sin las credenciales del usuario de las claves privadas de los suscriptores generadas en HSM y custodiadas de manera segura. La clave privada es única y es cifrada/descifrada por una clave sólo conocida y custodiada en el HSM. Sólo el suscriptor dispone de los mecanismos para su uso.
Almacenamiento de la clave privada	Las claves privadas de los suscriptores contenidas en archivos PKCS #12 NUNCA son almacenadas por ICERT-EC. El archivo PKCS #12 se envía al suscriptor para que éste lo almacene y conserve.	Las claves privadas de los suscriptores generadas en HSM son almacenadas en una base de datos del SFC en un blob cifrado mediante una clave solamente conocida por el HSM y activable sólo por el suscriptor. Para utilizar la clave privada del suscriptor es necesario descifrarla mediante una autenticación utilizando credenciales que sólo el suscriptor posee.

Transferencia de la clave privada	La clave privada de los suscriptores se encuentra dentro del archivo PKCS #12, el cual se envía por correo electrónico al suscriptor. En un correo electrónico adicional se envía la contraseña de dicho PKCS#12. El archivo PKCS #12 protege el uso de la clave privada a través de una clave que es custodiada por el suscriptor.	La clave privada de los suscriptores generada en el HSM nunca sale del propio HSM descifrada. Siempre que la clave privada viaja fuera del HSM está cifrada, y sólo el HSM puede descifrarla mediante credenciales que sólo el suscriptor posee.
Activación de la clave privada	La activación del archivo PKCS #12 que contiene la clave privada del suscriptor se realiza a través de una clave generada aleatoriamente y comunicada al suscriptor por correo electrónico.	La activación del uso de la clave privada generada en el HSM la realiza el suscriptor mediante la introducción de sus propias credenciales.
Desactivación de la clave privada	El método para desactivar la clave privada del suscriptor que ha importado su certificado a partir de un PKCS #12 es retirar el certificado del almacén de certificados que lo contenga, inmediatamente cualquier contenido asociado queda deshabilitado incluyendo la clave privada.	El método para desactivar la clave privada del suscriptor es mediante el cierre de sesión abierta con el SFC.
Destrucción de clave privada	La destrucción de la clave privada del suscriptor se realiza mediante la eliminación de la clave privada del almacén de certificados donde se encuentre y la destrucción de todas las copias del archivo PKCS #12	La destrucción de la clave privada se realiza mediante la eliminación del certificado asociado y mediante la eliminación de la propia clave.

6.2.1 Estándares para los módulos criptográficos

Las tarjetas criptográficas con certificados de firma electrónica, aptas como dispositivos seguros de creación de firma, contarán con la certificación FIPS del NIST Nivel 3 y/o Common Criteria EAL4+.

6.2.2 Control multipersona (k de n) de la clave privada

Las claves privadas de los certificados de departamento de empresa o institución no se encuentran bajo control de varias personas o multipersona. El control de dicha clave privada le corresponde únicamente al titular.

6.2.3 Custodia de la clave privada

La custodia de la clave privada de los certificados de departamento de empresa o institución está bajo el exclusivo control de sus titulares.

6.2.4 Copia de seguridad de la clave privada

En ningún caso se podrá realizar copia alguna de seguridad de las claves privadas de firma electrónica de departamento de Empresa o Institución.

6.2.5 Archivo de la clave privada

Las claves privadas de certificados de departamento de empresa o institución contenidas en

archivos PKCS #12 de ningún modo serán archivadas o almacenadas por ICERT-EC y sólo el usuario suscriptor tendrá acceso a dichas claves.

Las claves privadas de certificados de departamento de empresa o institución en HSM SFC serán almacenadas de forma segura en donde sólo el usuario suscriptor tendrá acceso a dichas claves archivadas.

6.2.6 Transferencia de la clave privada a o desde el módulo criptográfico

En ningún caso será permisible transferir las claves privadas de firma de departamento de empresa o institución.

6.2.7 Almacenamiento de la clave privada en un módulo criptográfico

Las claves privadas de certificados de departamento de empresa o institución se almacenan en el dispositivo criptográfico en el momento de la generación de los certificados.

Las claves privadas de los suscriptores nunca son almacenadas por el ICERT-EC.

La clave privada debe ser almacenada por el propio suscriptor debido a que puede ser necesaria para descifrar la información histórica cifrada con la clave pública.

6.2.8 Método de activación de la clave privada

La activación de la clave privada la podrá efectuar el titular a través del uso de su PIN. La protección de los datos de activación es responsabilidad del suscriptor.

6.2.9 Método de desactivación de la clave privada

El método para desactivar la clave privada del suscriptor que ha importado su certificado a partir de un PKCS #12 es retirar el certificado del almacén de certificados que lo contenga, inmediatamente cualquier contenido asociado queda deshabilitado incluyendo la clave privada.

6.2.10 Método de destrucción de la clave privada

La destrucción de la clave privada del suscriptor se produce luego de que el certificado es revocado o caducado, y siempre y cuando el usuario haya destruido todas la copias del archivo PKCS #12. La destrucción de una clave privada está asociada y precedida por una revocación del certificado asociado a la clave si éste estuviese vigente.

6.2.11 Clasificación de los módulos criptográficos

Los módulos criptográficos utilizados cumplen el estándar FIPS 140-2 Nivel 3 y/o Common Criteria EAL4+ (CWA 14169).

6.3 Otros aspectos de administración del par de claves

6.3.1 Archivo de la clave pública

La AR de la ICERT-EC mantiene archivados todos los certificados digitales de departamento de empresa o institución, los cuales incluyen la clave pública durante el periodo estipulado en la DPC.

6.3.2 Periodos operativos del certificado y periodos de uso del par de claves

Los certificados de departamento de empresa o institución tendrán validez y estarán operativos mientras no se manifieste de forma explícita su revocación en una CRL.

El par de claves tiene vigencia mientras exista un certificado de departamento de empresa o institución válido que las sustente. Una vez que el certificado deje de tener validez las claves pierden valor legal.

El periodo de validez de los certificados de departamento de empresa o institución es de dos (2) años desde el momento de su emisión.

6.4 Datos de activación

6.4.1 Generación de datos de activación e instalación

En esta unidad se expone el mecanismo con el cual se generan los datos de activación del HSM SFC o del archivo PKCS#12 que almacenan el par de claves y el certificado del suscriptor.

Archivo PKCS#12

- En el momento de generación del archivo PKCS#12 compuesto por par de claves y certificado, el PIN calculado aleatoriamente se le envía por e-mail al suscriptor.
- La clave debe ser custodiada por el suscriptor de modo que no sea conocida por nadie más y se garantice el control exclusivo del archivo PKCS #12.

HSM-SFC

- En el momento de generación de claves y certificado en el SFC, se genera unas credenciales aleatoriamente y se envían al suscriptor por e-mail.
- Las credenciales son custodiadas por el suscriptor de modo que no sean conocidas por nadie más y se garantice el control exclusivo de la clave privada.

6.4.2 Protección de datos de activación

La protección de los datos de activación del archivo PKC#S12 o HSM SFC es responsabilidad del suscriptor, para esto se considerará lo siguiente:

- La clave del archivo PKCS#12 debe ser generada y no conocida por nadie excepto por el suscriptor.
- Las credenciales de activación del HSM SFC deben ser generadas y no conocidas por nadie excepto por el suscriptor.

6.5 Controles de seguridad informática

Con el objetivo de efectuar una adecuada vigilancia de la seguridad de los recursos informáticos y garantizar la confiabilidad de los servicios ofrecidos por la ICERT-EC, en la Declaración de Prácticas de Certificación se describen los controles de seguridad informática.

7. PERFILES DE CERTIFICADO, CRL Y OCSP

7.1 Contenido del certificado

El contenido de los certificados de departamento de empresa o institución es el siguiente:

CERTIFICADOS DE DEPARTAMENTO DE EMPRESA O INSTITUCIÓN		
Campos de certificado X.509 v3 (tbsCertificate)		
Descripción	**Componente**	**Valor**
Versión del certificado	**version**	v3
Número que identifica unívocamente al certificado	**serialNumber**	Número entero aleatorio de 20 bytes
Firma	**signature**	
Algoritmo usado por el CJ para firmar el certificado	algorithm	sha256withRSAEncryption
Emisor	**Issuer**	
	commonName (CN)	*ENTIDAD DE CERTIFICACION ICERT-EC* [1]
	organizationalUnitName (OU)	*SUBDIRECCION NACIONAL DE SEGURIDAD DE LA INFORMACION DNTICS* [1]
	organizationName (O)	*CONSEJO DE LA JUDICATURA* [1]
	localityName (L)	*DM QUITO* [1]
	countryName (C)	*EC*
Validez	**validity**	
	notBefore	Fecha y hora de emisión del certificado, codificado en UTCTime
	notAfter	Not Before + 2 años, codificado en UTC Time
Asunto	**subject**	
	commonName (CN)	Nombre del departamento de la empresa o institución [1]
	serialNumber	RUC de la empresa o institución [1 2]
	organizationName (O)	Razón social de la empresa o institución [1]
	localityName (L)	Ciudad del departamento de la empresa o institución [1]
	countryName (C)	*EC*
Clave pública del titular del certificado	**subjectPublicKeyInfo**	
	algorithm-algorithm	rsa Encryption
	subjectPublicKey	Clave pública RSA, con tamaño de 2048 bits

[1] Codificado en `utf8String`, con las letras en español en mayúsculas, sin tilde ni diéresis en las vocales.
[2] Solo caracteres numéricos

7.1.1 Número de versión

Todos los certificados de departamento de empresa o institución emitidos por la ICERT-EC sustentados en esta política se emiten bajo el estándar X.509 Versión 3.

7.1.2 Extensiones del certificado

Las extensiones incluidas en los certificados digitales de departamento de empresa o institución son las siguientes:

keyUsage	crítica
basicConstraints	no crítica
certificatePolicies	no crítica
subjectAltName	no crítica

Extensiones de certificado X.509 v3 (extensions)	
authorityKeyIdentifier	
keyIdentifier	Valor en extensión subjectKeyIdentifier del certificado de CA Subordinada CJ
subjectKeyIdentifier	Hash SHA-1 de la clave pública RSA en subjectPublicKey
keyUsage (critical)	digitalSignature nonRepudiation
certificatePolicies	
policyIdentifier	1.3.6.1.4.1.43745.1.2.3.1.x.y [4]
policyQualifiers	
policyQualifierId	id-qt-cps
qualifier-cPSuri	*http://www.icert.fje.gob.ec/dpc/declaracion_practicas_certificacion.pdf*
subjectAltName	
rfc822Name	E-mail de envío de notificaciones
directoryName	
1.3.6.1.4.1.43745.1.3.1	Número de cédula o pasaporte de la persona responsable del certificado (opcional)[12]
1.3.6.1.4.1.43745.1.3.2	Nombre(s) de la persona responsable del certificado (opcional)[1]
1.3.6.1.4.1.43745.1.3.3	Primer apellido de la persona responsable del certificado (opcional)[1]
1.3.6.1.4.1.43745.1.3.4	Segundo apellido de la persona responsable del certificado (opcional)[1]
1.3.6.1.4.1.43745.1.3.5	Cargo de la persona responsable del certificado (opcional)[2]
1.3.6.1.4.1.43745.1.3.7	Dirección del departamento de la empresa o institución[1]
1.3.6.1.4.1.43745.1.3.8	Teléfono del departamento de la empresa o institución[13]
1.3.6.1.4.1.43745.1.3.9	Ciudad del departamento de la empresa o institución[1]
1.3.6.1.4.1.43745.1.3.10	Razón social de la empresa o institución[1]
1.3.6.1.4.1.43745.1.3.11	RUC de la empresa o institución[12]
1.3.6.1.4.1.43745.1.3.12	País: *ECUADOR*[1]
1.3.6.1.4.1.43745.1.3.50	Tipo de titular de certificado: *DEPARTAMENTO DE EMPRESA O INSTITUCION*[1]
1.3.6.1.4.1.43745.1.3.51	Tipo de contenedor criptográfico (uno de los valores): *HARDWARE-HSM SFC*;

[1] Codificado en `utf8String`, con las letras en español en mayúsculas, sin tilde ni diéresis en las vocales.
[2] Alfanumérico mayúsculas en inglés.
[3] Sólo caracteres numéricos.
[4] Dependiendo del tipo de contenedor criptográfico: HARDWARE-HSM SFC `x=1 y=2`; SOFTWARE-ARCHIVO (PKCS#12) `x=2 y=1`

	SOFTWARE-ARCHIVO (PKCS#12)[1]
1.3.6.1.4.1.43745.1.3.54	Nombre del departamento de la empresa o institución[1]
basicConstraints	
extKeyUsage	id-kp-emailProtection
cRLDistributionPoints	
distributionPoint-fullName	
uniformResourceIdentifier	*http://www.icert.fje.gob.ec/crl/icert.crl*
authorityInfoAccess	
accessMethod	id-ad-ocsp
accessLocation -uniformResourceIdentifier	*http://ocsp.icert.fje.gob.ec*

7.1.3 Identificadores de objeto de los algoritmos

Los certificados digitales de Departamento de Empresa o Institución utilizan los siguientes algoritmos:

- Algoritmo de firma SHA withRSA Encryption
- Algoritmo de la clave pública SHA 256 with RSA Encryption

7.1.4 Formatos de nombre

Los certificados digitales de Departamento de Empresa o Institución emitidos por la ICERT-EC contienen el distinguished name X.500 del emisor y del titular del certificado en los campos issuer name y subject name respectivamente.

7.1.5 Restricciones de nombre

Los nombres contenidos en los certificados emitidos bajo esta política están restringidos a "Distinguished Names" X.500, que son únicos.

7.1.6 Identificador de la Política de Certificados

La presente Política de Certificados de Departamento de Empresa o Institución está signada mediante el número único OID *1.3.6.1.4.1.43745.1.2.3.1*

7.1.7 Sintaxis y semántica de los calificadores de la política

El contenido de la extensión de los certificados referente a los calificadores de la Política de Certificados contiene la siguiente información:

- **policyIdentifier:** Contiene el identificador de la Política de Certificados de Departamento de Empresa o Institución.
- **URL DPC**: contiene la URL donde se puede obtener la última versión de la DPC y PC asociada.

7.2 Perfil de la CRL

7.2.1 Número de versión

La infraestructura de Clave Pública del Consejo de la Judicatura utiliza CRL X.509 versión 2.

7.2.2 CRL y extensiones

De conformidad a lo prescrito en las sección 7.2.2 de la Declaración de Prácticas de Certificación de la ICERT-EC.

7.3 Perfil OCSP

7.3.1 Numero de versión

El certificado OCSP de la ICERT-EC se emite de acuerdo al estándar X.509 V3.

7.3.2 Extensiones OCSP

Las extensiones OCSP según estándar X.509Versión 3, de la ICERT-EC son las siguientes:

keyUsage	crítica
basicConstraints	crítica

Código:	Sustituye a:	Fecha de emisión:	Fecha de revisión:
00-11-A.05-POL3.0-7Política de Certificados de Departamento de Empresa o Institución	00-11-A.05-POL2.0-7Política de Certificados de Departamento de Empresa o Institución	Octubre 2014	Septiembre 2016

8. AUDITORIA DE CUMPLIMIENTO Y OTRAS VALORACIONES

En la Declaración de Prácticas de Certificación de la ICERT-EC se establece la información sobre la auditoria y otras valoraciones.

9. OTROS NEGOCIOS Y ASUNTOS LEGALES

9.1 Tarifas

Las tarifas por emisión de certificados digitales se publican en la página web del Consejo de la Judicatura en la siguiente ubicación: http://www.icert.fje.gob.ec sección tarifas.

9.2 Responsabilidad financiera

Se establece en la Declaración de Prácticas de Certificación de la ICERT-EC.

9.3 Confidencialidad de la información

Se establece en la Declaración de Prácticas de Certificación de la ICERT-EC.

9.4 Protección de la información personal

Se establece en la Declaración de Prácticas de Certificación de la ICERT-EC.

9.5 Derechos de propiedad intelectual

Se establece en la Declaración de Prácticas de Certificación de la ICERT-EC.

9.6 Obligaciones y garantías

En la Declaración de Prácticas de Certificación se detallan las obligaciones y garantías por parte de la Autoridad de Certificación de la ICERT-EC, las Autoridades de Registro, los solicitantes, suscriptores y usuarios del servicio de certificación.

9.7 Limitaciones de responsabilidad

Se establece en la Declaración de Prácticas de Certificación de la ICERT-EC.

9.8 Indemnizaciones

Se establece en la Declaración de Prácticas de Certificación de la ICERT-EC.

9.9 Duración y terminación

Se establece en la Declaración de Prácticas de Certificación de la ICERT-EC.

9.10 Procedimiento de cambio en las especificaciones

Se establece en la Declaración de Prácticas de Certificación de la ICERT-EC.

9.11 Prevención de disputas

Se establece en la Declaración de Prácticas de Certificación de la ICERT-EC.

9.12 Ley aplicable

Se establece en la Declaración de Prácticas de Certificación de la ICERT-EC.

9.13 Estipulaciones diversas

9.13.1 Cláusula de aceptación completa

Se establece en la Declaración de Prácticas de Certificación de la ICERT-EC.

9.13.2 Independencia

En el caso de que una o más estipulaciones de esta Política de Certificados sean o llegasen a ser inválidas, nulas, o inexigibles legalmente, se entenderán como no incluidas, salvo que dichas estipulaciones fueran esenciales de manera que al excluirlas de la PC careciera ésta de toda eficacia jurídica.