ENTIDAD DE CERTIFICACIÓN DEL CONSEJO DE LA JUDICATURA

ICERT-EC

POLÍTICA DE CERTIFICADOS

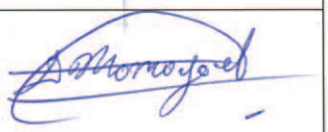
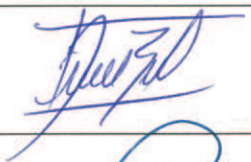
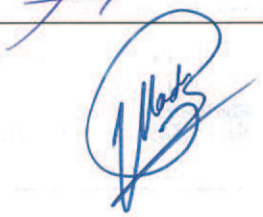
Certificado de Funcionario Público

ICERT - EC ENTIDAD DE CERTIFICACIÓN Consejo de la Judicatura	***POLÍTICA DE CERTIFICADOS DE FUNCIONARIO PÚBLICO***	*Versión: 2.0*
		Fecha: 17-10-2014
		OID: 1.3.6.1.4.1.43745.1.2.1.5

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.

Firmas de responsabilidad

	Nombre	Cargo	Firma
Creado por:	David Moncayo	Experto en Proyectos DNTICs	
Creado por:	Flor Chancay	Analista 4 DNTICs	
Revisado por:	José Luis Medina	Subgerente de Proyectos DNTICs	
Aprobado por:	Vladimir Rodríguez	Subdirector Nacional de Infraestructuras, Servicios y Telecomunicaciones Administrador del Contrato 133-2013	

CONTENIDO

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 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 y Servicios Relacionados.

1.1 Presentación general del documento

La presente Política de Certificados (PC) de Funcionario Público, se ajusta y complementa con 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 Funcionario Público, de conformidad a lo establecido en el Acuerdo Ministerial No. 181 de 15 de septiembre de 2011, del Ministerio de Telecomunicaciones y de la Sociedad de la Información, "son certificados que identifican al suscriptor como funcionario o servidor público, quien actuará a título de la Institución pública que representa y será responsable de todo lo que firme electrónicamente dentro del ámbito de su actividad y límites de uso que correspondan".

1.2 Nombre del documento e identificación

Este documento se denomina Política de Certificados de Funcionario Público, 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_funcionario_publico.pdf

Nombre del documento	*POLITICA DE CERTIFICADOS* *Certificado de Funcionario Público*
Descripción	*Los certificados de Funcionario Público acreditan la identidad del suscriptor y le permiten firmar documentos electrónicamente con la misma validez legal que la firma manuscrita.*
Identificador OID	*1.3.6.1.4.1.43745.1.2.1.5*
Versión	*2.0*
Fecha de emisión	*17 de octubre de 2014*
Ubicación	http://www.icert.fje.gob.ec/dpc/pc_funcionario_publico.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. Los Certificados de Funcionario Público emitidos por la ICERT-EC tienen asignados los siguientes identificadores de objeto (OID) dependiendo del tipo de contenedor criptográfico:

- Certificado de Funcionario Público

  1.3.6.1.4.1.43745.1.2.1.5

- Certificado de Funcionario Público - Hardware

  1.3.6.1.4.1.43745.1.2.1.5.1

- Certificado de Funcionario Público - Hardware - Token/Tarjeta

  1.3.6.1.4.1.43745.1.2.1.5.1.1

- Certificado de Funcionario Público - Hardware –HSM SFC

  1.3.6.1.4.1.43745.1.2.1.5.1.2

- Certificado de Funcionario Público - Software

  1.3.6.1.4.1.43745.1.2.1.5.2

- Certificado de Funcionario Público - Software - Archivo (PKCS #12)

  1.3.6.1.4.1.43745.1.2.1.5.2.1

1.4 Dispositivos para certificados de Funcionario Público

Los dispositivos para Certificados de Funcionario Público pueden ser de varios tipos, de conformidad con el contenedor criptográfico:

- Certificado en dispositivo criptográfico de tipo HW-token/tarjeta.
- Certificado en archivo SW-PKCS#12.
- Certificado en Hardware Dispositivo criptográfico de tipo HSM SFC.

1.5 Administración de la Política de Certificados de Funcionario Público

La Política de Certificados de Funcionario Público es administrada por la Subdirección Nacional de Seguridad de la Información, encargada de su elaboración, actualización, registro y mantenimiento.

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

1.5.1 Entidad que administra el certificado

NOMBRE	*Subdirección Nacional de Seguridad de la Información*
DIRECCIÓN	*Av. 12 de Octubre N24-593 y Francisco Salazar*
TELÉFONO	*(02) 395 3 600*
Email	entidad.certificacion@funcionjudicial.gob.ec

1.5.2 Persona de contacto

ENTIDAD DE CERTIFICACIÓN	*Entidad de Certificación ICERT – EC*
NOMBRE	*Ing. Reynaldo Gaibor* *Sub Director Nacional de Seguridad de la Información*
DIRECCIÓN	*Av. 12 de Octubre N24-593 y Francisco Salazar*
TELÉFONO	*(02) 3953 600*
Email	entidad.certificacion@funcionjudicial.gob.ec

1.5.3 Procedimiento para aprobación de la política

La Política de Certificados de Funcionario Público 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 Funcionario Público es un documento público que se encuentra disponible en la página http://www.icert.fje.gob.ec/dpc/pc_funcionario_publico.pdf de la ICERT-EC. Las modificaciones a estas políticas, que fueren aprobadas de acuerdo al procedimiento previsto se publicarán de forma inmediata.

1.6 Entidades y personas participantes

Los certificados de Funcionario Público son emitidos a las personas físicas que documentan su identidad como funcionario o servidor de una entidad del Estado ecuatoriano 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 Funcionario Público interviene con voluntad en su nombre 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 para Funcionario Público de conformidad con los términos establecidos en ésta 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 la 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 para Funcionario Público.

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 digitales requiriendo la emisión de los certificados a la AC Subordinada.

Está facultada además para solicitar a la AC Subordinada la revocación, suspensión y rehabilitación 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 Funcionario Público.

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

1.6.3 Solicitante

El solicitante es aquella persona natural que a nombre propio, o con representación legal del titular, desea acceder a los servicios de certificación digital al adquirir un certificado de Funcionario Público emitido por la ICERT-EC.

En ningún caso se aceptarán solicitudes de este tipo de certificados a nombre de personas que no demuestren su legítima representación.

1.6.4 Suscriptor

El suscriptor es aquella persona física a quien se le otorga un certificado de Funcionario Público 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 voluntariamente deciden confiar y aceptar en un certificado para Funcionario Público 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 Funcionario Público tendrán una validez de dos (2) años

1.7.2 Uso apropiado de los certificados

El certificado de Funcionario Público 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 Funcionario o Servidor Público ante servicios y aplicaciones informáticas, confirmando su autenticidad e integridad.

1.7.2.2 Firma digital

Las firmas digitales efectuadas con certificados de Funcionario Público 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 ser 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 mismo, 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 Funcionario Público 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 Funcionario Público 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.
- Se prohíbe el uso de certificados que puedan ocasionar daños personales o medioambientales.
- Se considera prohibida 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 en el certificado.

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.

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

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.

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).

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.

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 claves públicas que especifica entre otros temas, los formatos estándar para certificados de claves públicas y para la implementación de listas de certificados en revocación.

1.12 Siglas

AC:	**A**utoridad de **C**ertificación
AD	(**A**ctive **D**irectory): **D**irectorio Activo
AR:	**A**utoridad de **R**egistro
API	**A**pplication **P**rogramming **I**nterface
ARL	**A**uthority **R**evocation **L**ist
ASCII	**A**merican **S**tandard **C**ode for **I**nformation **I**nterchange
ASN.1	**A**merican **S**tandard **C**ode for **I**nformation **I**nterchange
AV:	**A**utoridad de **V**alidación
BD	**B**ase de **D**atos
C	**C**ountryName
CA	**C**ertification **A**uthority (Autoridad de Certificación AC)
CAdES	**C**MS **A**dvanced **E**lectronic **S**ignatures
CAdES- XL	**C**MS **A**dvanced **E**lectronic **S**ignatures e**X**tended **L**ong-term
CEN	**C**omité **E**uropéen de **N**ormalisation
CJ	**C**onsejo de la **J**udicatura
CN	**C**ommon**N**ame
CMS	**C**ontent **M**anagement **S**ystem
cps	**c**ertificate **p**ractice **s**tatement
CRL	**C**ertificate **R**evocation **L**ist (Lista de certificados revocados)

CSP	Cryptographic Service Provider
CSR	Certificate Signing Request
CSV	Comma-Separated Values
CWA	CEN Workshop Agreement
DD	Day Day
DIT	Directory Information Tree
DN	Distinguished Name
DNS	Domain Name System
DPC	Declaración de Prácticas de Certificación
DNTIC's:	Dirección Nacional de Tecnologías de la Información y Comunicaciones
EAL4+	Evaluation Assurance Level 4+
FC	Firma Centralizada
FIFO	First In First Out
FIPS	Federal Information Processing Standards
GMT	Greenwich Mean Time
hh	hour hour
HSM	Hardware Security Module (Módulo de Seguridad Criptográfica)
HTTP	Hypertext Transfer Protocol
HTTPS	HTTP Secure
ICERT-EC	Entidad de Certificación del Consejo de la Judicatura
INOCAR	INstituto OCeanográfico de la ARmada
IP	Internet Protocol
ISO	International Organization for Standardization
kp	key purpose
L	LocalityName
LDAP	Lightweight Directory Access Protocol
MIME	Multipurpose Internet Mail Extensions
MM	Month Month
mm	minute minute
NTP	Network Time Protocol
O	OrganizationName
OCSP	Online Certificate Status Protocol (Protocolo de estatus de certificados en línea)
OID	Object Identifier (Identificador de Objetos)
OU	OrganizationalUnitName
PAdES	PDF Advanced Electronic Signature
PAdES-LTV	PAdES Long Term Validation
PC	Política de Certificados
PDF	Portable Document Format
PDF/A	PDF/Archive

PEM	Privacy Enhanced Mail
PIN	Personal Identification Number
PKCS	Public-Key Cryptography Standard (Estándares de criptografía de clave pública)
PKI	Public Key Infrastructure (Infraestructura de Clave Pública)
RA	Registration Authority (Autoridad de Registro AR)
RAID	Redundant Array of Independent Disks
RFC	Request For Comments (Petición de comentarios)
RSA	Rivest Shamir Adleman
RTF	Rich Test Format
RUC	Registro Único de Contribuyentes
SAM	Security Accounts Manager
SFC	Servidor de Firma Centralizada
SHA	Secure Hash Algorithm
S/MIME	Secure MIME
SMTP	Simple Mail Transfer Protocol
SNMP	Simple Network Management Protocol
SPKC	Signed Public Key and Challenge
SQL	Structured Query Language
ss	second second
SSL	Secure Socket Layer
SSH	Secure SHell
TCP	Transmission Control Protocol
TLS	Transport Layer Security
TSA	Time-Stamping Authority
TSP	Time-Stamp Protocol
TWS	Trust Worthy System
UDP	User Datagram Protocol
UML	Unified Modeling Language
URI	Uniform Resource Identifier
UTC	Universal Time Coordinated
UTF-8	8-bit Unicode Transformation Format
v	version
VA	Validation Authority (Autoridad de Validación AV)
VT100	Video Terminal 100
XADES	XML Advanced Electronic Signatures
XADES- XL	XML Advanced Electronic Signatures eXtended Long-term
YY	Year Year
YYYY	Year Year Year Year

2. PUBLICACIÓN Y REGISTRO DE CERTIFICADOS

Las Políticas de Certificados (PC), 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 la ICERT-EC 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 de las mismas.

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 Autoridad de Certificación de la ICERT-EC en el momento de autenticar la identidad del solicitante y aprobar la emisión de un certificado de Funcionario Público.

3.1 Registro inicial

Previo a la emisión inicial de un Certificado para Funcionario Público, 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 de un suscriptor de certificados, 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 Funcionario Público tienen una sección llamada Subject cuyo objetivo es permitir identificar al suscriptor o titular del certificado, incluyendo un atributo 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 para Funcionario Público*
CN	Nombre común	*Nombres y apellidos completos del suscriptor*

3.2.2 Necesidad de que los nombres sean significativos

Todo certificado de Funcionario Público 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 seudónimos en los nombres

De acuerdo a esta Política de Certificados no se admiten anónimos ni seudónimos para identificar el nombre de un Funcionario Público.

En el caso de un Funcionario Público con nacionalidad ecuatoriana, el nombre debe estar conformado por nombres y apellidos tal como consta en la cédula de ciudadanía. Si el Funcionario Público es un extranjero, el nombre debe estar conformado por nombres y apellidos tal como consta en el pasaporte.

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 Funcionarios Públicos están escritos utilizando lenguaje natural, prescindiendo de acentos. En ningún caso se pueden modificar los nombres y apellidos de un Funcionario Público, 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 Funcionario Público 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

Las claves del certificado de Funcionario Público serán generadas por el titular de dicho certificado; para demostrar que el titular posee la clave privada correspondiente a la clave pública que se pretende vincular al certificado de Funcionario Público, se probará mediante el envío de la petición de certificado, en la cual se incluirá la clave pública firmada mediante la clave privada asociada.

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

a) Generación en Token o Tarjeta criptográfica

La AR permite realizar al operador de emisión la generación del par de claves de firma en el Token/Tarjeta criptográfica y del certificado emitido por la AC.

Completado dicho procedimiento, es posible descargar el certificado en formato PEM directamente desde el Token/Tarjeta criptográfica.

Una vez finalizado el proceso, la AR envía al suscriptor el PIN del Token/Tarjeta criptográfica por correo electrónico. El PIN establecido es calculado a través de algoritmos y completamente desconocido para terceras partes.

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

b) 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.

c) Generación en HSM SFC y custodia segura remota

La AR 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 lógica.

3.3.2 Autenticación de la identidad de Funcionario Público

El solicitante para demostrar su identidad debe proporcionar la siguiente información y documentación para adquirir el certificado de Funcionario Público, de conformidad a la normativa aplicable y al cuadro de identificadores de campo:

NUMERO IDENTIFICADOR	CAMPOS
3.1	*Cédula o Pasaporte del suscriptor*
3.2	*Nombres del suscriptor*
3.3	*Primer apellido del suscriptor*
3.4	*Segundo apellido del suscriptor (si no tiene no aparece dentro del certificado)*
3.5	*Cargo*
3.6	*Dirección*
3.7	*Teléfono*
3.8	*Ciudad*
3.9	*País*
3.12	*Cédula o Pasaporte del suscriptor*

3.11	***RUC de la Institución***
3.10	***Razón Social***

La información suministrada por el solicitante a través de la página web, será revisada por la Autoridad de Registro quien se encarga 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 Funcionario Público el solicitante debe proporcionar documentos y datos que lo identifican absolutamente, toda la información solicitada es 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. También puede ser procesada mediante una solicitud enviada por un tercero debidamente identificado que represente al suscriptor. Así mismo también es posible mediante una identificación física en la Autoridad de Registro, por la que el operador de reconocimiento procederá a la revocación.

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

Los certificados de Funcionario Público 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 certificado de Funcionario Público la puede realizar cualquier persona mayor de edad que demuestre ser Funcionario o Servidor Público, que se encuentre autorizado por la institución estatal para actuar en nombre de la misma en función del cargo que representa y que esté en plena capacidad para contratar y obligarse de cumplir con las responsabilidades inherentes al uso de este certificado.

4.1.2 Presentación de una solicitud de certificado

Todo Funcionario Público que desee obtener un Certificado de Firma Electrónica emitida por la ICERT-EC, debe llenar el formulario de solicitud de Certificado y presentarlo a la Autoridad de Registro de la ICERT-EC, a través de la página web.

4.1.3 Comprobación de solicitudes

La Autoridad de Registro de la ICERT-EC deberá comprobar y validar la información y los documentos que son requeridos para solicitar los certificados de Funcionario Público.

Para estos efectos el solicitante autoriza y faculta expresamente a la ICERT-EC y a su Autoridad de Registro, verifiquen los antecedentes entregados 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 realizada para la emisión de los certificados de Funcionario Público, por un período de mínimo cinco (5) años.

4.1.4 Proceso de solicitud de certificados y responsabilidades de los solicitantes

El procedimiento que debe realizar el peticionario para la emisión de un certificado de Funcionario Público es el siguiente:

No.	Responsable	Descripción de la actividad	Documentos de apoyo
1	Usuario Suscriptor	Ingresar solicitud a través de la web	Documentos escaneados
2	Asistente Administrativo 1	Revisar solicitudes, aprueba o archiva las solicitudes (Si fue aprobada se notifica al usuario el valor a pagar por tipo de solicitud)	Documentos escaneados

3	Asistente Administrativo 1	A través del sistema se archiva solicitudes aprobadas de las que no se ha hecho el pago en más de 30 días	

Es responsabilidad del solicitante garantizar la veracidad de toda la información proporcionada para obtener sus certificados de Funcionario Público. La ICERT-EC podrá verificar que los datos proporcionados por el solicitante son fidedignos.

La ICERT-EC en función de sus actividades, garantizará el derecho a la protección de datos de carácter personal, que incluye el acceso y la decisión sobre información y datos de ese carácter, así como su correspondiente protección.

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 sin expresión de causa ni motivación, las solicitudes que no cumplan con los requerimientos, información y documentación solicitados en la presente Política de Certificados de Funcionario Público, o que los documentos presentados no sean concordantes. El archivo de la solicitud 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 la Autoridad de Registro su comprobante de pago, el mismo que se ingresará en el sistema con la generación de la factura correspondiente. Una vez realizado el pago el usuario tiene un tiempo de treinta (30) días para acercarse a la emisión, 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 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	Asistente Administrativo 2	Revisa que no haya caducado su pago para el certificado a emitir	
2	Usuario Suscriptor	Entrega de documentación al operador para revisión	
3	Asistente Administrativo 2	Valida y actualiza información, confirmada la información realiza la toma de una fotografía y realiza la firma de la solicitud	Solicitud
4	Usuario Suscriptor	Revisa la solicitud del certificado, la firma y la entrega al Asistente Administrativo	Solicitud firmada
5	Asistente Administrativo 2	Recepta la solicitud firmada, la archiva en papel y/o digital, y entrega una copia sellada al usuario	Solicitud firmada y sellada
6	Asistente Administrativo 2	Emite el certificado	
7	Asistente Administrativo 2	Genera el contrato y entrega el certificado al Usuario	
8	Usuario Suscriptor	El usuario firma el contrato	
9	Asistente Administrativo 2	Almacena el contrato y lo envía vía correo	Contrato firmado electrónicamente

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 Funcionario Público que suscribe la misma.

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 los titulares de los certificados expresan la aceptación de los términos y condiciones contenidos en el contrato de aceptación de condiciones de los servicios de certificación que otorga 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 Funcionario Público 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 Funcionario Público. 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 esta PC, y sólo para la realización de funciones que requieran acreditar la identidad del titular como Funcionario Público.

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 Funcionario Público, 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 el mismo 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 3 meses, 2 meses, 1 mes, 2 semanas, 1 semana y 1 día de 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 para Funcionario Público, 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 mismos.

4.6.1 Situaciones 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 pedir la renovación de los certificados?

La renovación de los certificados de Funcionario Público, únicamente puede ser solicitada por el titular de los mismos 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 para Funcionario Público, 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 Funcionario Público.

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, suspensión y rehabilitación 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 rehabilitación de un certificado desde la AR puede ser realizada manualmente 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 rehabilitado, 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 misma 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 para la caducidad del certificado.

4.9 Servicios de información del estado de 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 Funcionario Público se especifica la validez plena y legal del mismo, ya que se determina desde y hasta cuando está vigente.

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 se encuentran protegidos contra toda alteración que 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 Dispositivo Token/Tarjeta criptográfica 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).
- 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 digital que se emite en dispositivo Token/Tarjeta criptográfica la clave privada la genera el operador de RA en el dispositivo bajo la presencia del suscriptor, y su uso es protegido mediante un PIN.

Para el formato PKCS#12 la clave privada se encuentra contenida en el archivo y se enviará en por email al suscriptor. En otro email 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 RA 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 del certificado

El mecanismo de entrega de la clave pública a titulares de Certificados para Funcionario Público

varía si la forma de entrega es en dispositivo Token/Tarjeta criptográfica, en archivo con formato PKCS#12 o en HSM SFC.

La clave pública de los certificados para Funcionario Público se genera en el dispositivo criptográfico del titular 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 del 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 Funcionario Público 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 Funcionario Público 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 Funcionario Público 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 Protección de la clave privada

En el cuadro siguiente se especifican los controles de protección de la clave privada del suscriptor según la forma de entrega del certificado:

Control de la ICERT-EC para protección de la clave privada	Forma de entrega del certificado		
	Dispositivo Token/Tarjeta criptográfica	Archivo PKCS #12	HSM SFC

Respaldo de la clave privada	ICERT-EC no realiza respaldo sobre las claves privadas de los suscriptores generadas desde dispositivo TOKEN. ICERT-EC nunca está en posesión de dichas claves y solo permanecen bajo custodia del propio suscriptor	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 generadas en dispositivo Token o Tarjeta criptográfica NUNCA son almacenadas por ICERT-EC. La clave privada debe ser almacenada por el propio suscriptor mediante la conservación del dispositivo TOKEN u otros métodos, debido a que pueden ser necesarias para descifrar la información histórica cifrada con la clave pública.	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 generada en TOKEN/Tarjeta criptográfica nunca sale del propio dispositivo/contenedor. Con el dispositivo Token/Tarjeta criptográfica se genera el par de claves y se protege su uso a través de un PIN que solo conoce el suscriptor.	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 dispositivo Token/Tarjeta criptográfica que contiene la clave privada del suscriptor se realiza a través de un PIN generado aleatoriamente y comunicado al suscriptor por correo electrónico, La protección de los datos de activación es responsabilidad del suscriptor.	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 protección de los datos de activación es responsabilidad exclusiva del suscriptor.	La activación del uso de la clave privada generada en el HSM la realiza el suscriptor mediante la introducción de sus propias credenciales. La protección de los datos de activación es responsabilidad del suscriptor.

Desactivación de la clave privada	El método para desactivar la clave privada del suscriptor es retirar el dispositivo Token/Tarjeta criptográfica del equipo, inmediatamente cualquier contenido asociado queda deshabilitado incluyendo 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 dentro de un dispositivo Token/Tarjeta criptográfica es a través de la eliminación de los certificados y claves incluidos en el dispositivo criptográfico.	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 es 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 para firma electrónica, aptas como dispositivos seguros de creación de firma, contarán con la certificación FIPS 140-2 del NIST Nivel 3 y/o Common Criteria EAL4+.

6.2.2 Control multipersona de la clave privada

Las claves privadas de los certificados de Funcionario Público 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 Funcionario Público está bajo el exclusivo control de los titulares de las mismas.

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 Funcionario Público.

6.2.5 Archivo de la clave privada

Las claves privadas de firma de Funcionario Público en dispositivos criptográficos Token/Tarjeta criptográfica de ningún modo serán archivadas para garantizar el no repudio.

Las claves privadas de firma de Funcionario Público contenidas en archivos PKCS #12 de ningún modo serán archivadas o almacenadas por ICERT-EC.

Las claves privadas de firma de Funcionario Público 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 Funcionario Público. La clave privada de los suscriptores generada desde el Token/Tarjeta criptográfica nunca sale del dispositivo.

6.2.7 Almacenamiento de la clave privada en un módulo criptográfico

Las claves privadas de firma para Funcionario Público se almacenan en el dispositivo criptográfico en el momento de la generación de los certificados.

Las claves privadas de los suscriptores generadas desde el dispositivo Token/Tarjeta criptográfica nunca son almacenadas por el ICERT-EC.

La clave privada debe ser almacenada por el propio suscriptor mediante la conservación del dispositivo Token/Tarjeta criptográfica u otros métodos, debido a que pueden ser necesarias 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 es retirar el dispositivo Token/Tarjeta criptográfica del equipo, 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 Funcionario Público, los cuales incluyen la clave pública durante el periodo estipulado en la DPC.

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

Los certificados de Funcionario Público 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 Funcionario Público 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 Funcionario Público es de dos (2) años desde el momento de emisión del mismo.

6.4 Datos de activación

6.4.1 Generación de datos de activación e instalación

En esta sección se expone el mecanismo con el cual se generan los datos de activación del dispositivo Token/Tarjeta criptográfica, HSM SFC o del archivo PKCS#12 que almacenan el par de claves y el certificado del suscriptor.

Dispositivo TOKEN

- En el momento de generación de claves e importación del certificado, el PIN por defecto del Token/Tarjeta criptográfica se cambian aleatoriamente y se le envían por email al suscriptor. El suscriptor podrá cambiar el PIN del dispositivo siempre que lo considere oportuno.
- El PIN debe ser custodiado por el suscriptor de modo que no sea conocido por nadie más y se garantice el control exclusivo del TOKEN.

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 email 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 email.
- Las credenciales son custodiadas por el suscriptor de modo que 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 dispositivo Token/Tarjeta criptográfica, archivo PKCS#12 o HSM SFC son de responsabilidad del suscriptor, para esto se considerará lo siguiente:

- La clave de activación del TOKEN debe ser cambiada y no conocida por nadie excepto por el suscriptor. El suscriptor podrá cambiar la clave del TOKEN/Tarjeta criptográfica.
- 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 debe ser generada y no conocida 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 Funcionario Público es el siguiente:

CERTIFICADOS DE FUNCIONARIO PÚBLICO		
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)	*SUBDIRECCIÓN 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 y apellidos del funcionario público
	serialNumber	Número de cédula o pasaporte del funcionario público
	organizationName (O)	Razón social de la institución
	localityName (L)	Ciudad del departamento de la institución
	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] Sustituir por el mismo dato de la institución, si no se quieren incluir datos del departamento en los certificados.

7.1.1 Número de versión

Todos los certificados de Funcionario Público 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 Funcionario Público 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	1.3.6.1.4.1.43745.1.2.1.5.x.y [3]
policyQualifiers	
policyQualifierId	id-qt-cps
qualifier-cPSuri	*http://www.icert.fje.gob.ec/dpc/declaracion_practicas_certificacion.pdf*
subjectAltName	
rfc822Name	E-mail del funcionario público
directoryName	
1.3.6.1.4.1.43745.1.3.1	Número de cédula o pasaporte del funcionario público [4]
1.3.6.1.4.1.43745.1.3.2	Nombre(s) del funcionario público[1]
1.3.6.1.4.1.43745.1.3.3	Primer apellido del funcionario público[1]
1.3.6.1.4.1.43745.1.3.4	Segundo apellido del funcionario público (opcional)[1]
1.3.6.1.4.1.43745.1.3.5	Cargo del funcionario público[1]
1.3.6.1.4.1.43745.1.3.6	Nombre del departamento de la institución[12]
1.3.6.1.4.1.43745.1.3.7	Dirección del departamento de la institución[12]
1.3.6.1.4.1.43745.1.3.8	Teléfono del departamento de la institución[123]
1.3.6.1.4.1.43745.1.3.9	Ciudad del departamento de la institución[12]
1.3.6.1.4.1.43745.1.3.10	Razón social de la institución[123]
1.3.6.1.4.1.43745.1.3.11	RUC de la institución[123]
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: *FUNCIONARIO PUBLICO*[1]
1.3.6.1.4.1.43745.1.3.51	Tipo de contenedor criptográfico (uno de los valores): *HARDWARE-TOKEN/TARJETA; HARDWARE-HSM SFC; SOFTWARE-ARCHIVO (PKCS#12)*[1]
1.3.6.1.4.1.43745.1.3.52	RUP de la institución (opcional)[1]
basicConstraints	
extKeyUsage	id-kp-clientAuth 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*

[1] Codificado en utf8String, con las letras en Español en mayúsculas, sin tilde ni diéresis en las vocales

[2] Sustituir por los datos de departamento o de institución de ser el caso cuando no posea datos de departamento

[3] Solo caracteres numéricos

[4] Alfanumérico mayúsculas en Inglés

7.1.3 Identificadores de objeto de los algoritmos

Los certificados digitales de Funcionario Público utilizan los siguientes algoritmos:

- Algoritmo de firma SHA1withRSA Encryption
- Algoritmo de la clave pública SHA-256 with RSA Encryption

7.1.4 Formatos de nombre

Los Certificados digitales de Funcionario Público 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 y no ambiguos.

7.1.6 Objeto identificador de la Política de Certificados

La presente Política de Certificados de Funcionario Público está signada mediante el número único OID 1.3.6.1.4.1.43475.1.2.1.5.

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:

- **Policy identifier:** Contiene el identificador de la Política de Certificados de Funcionario Público.
- **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 CRLs X.509 v2.

7.2.2 CRL y extensiones

De conformidad a lo prescrito en las secciones 7.1 y 7.2.2 de la Declaración de Prácticas de Certificación del Consejo de la Judicatura.

7.3 Perfil OCSP

7.3.1 Numero de versión

El certificado OCSP del Consejo de la Judicatura se emite de acuerdo al estándar X.509 v3.

7.3.2 Extensiones OCSP

Las extensiones OCSP según estándar X.509 v3, de la ICERT-EC son las siguientes:

keyUsage	crítica
basicConstraints	crítica

8. AUDITORIA DE CONFORMIDAD 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, la Autoridad 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 Certificación sean o llegasen a ser inválidas, nulas, o inexigibles legalmente, se entenderá por no puesta, salvo que dichas estipulaciones fueran esenciales de manera que al excluirlas de la PC careciera ésta de toda eficacia jurídica.