ENTIDAD DE CERTIFICACIÓN DEL CONSEJO DE LA JUDICATURA ICERT-EC

DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN

SUBDIRECCIÓN NACIONAL DE SEGURIDAD DE LA INFORMACIÓN

JEFATURA DE FIRMA ELECTRÓNICA

FECHA: 14/05/2024

Código:	JFE-SNS-2024-020-CF
Versión:	5.0
Fecha de elaboración	14/05/2024
Elaborado por:	Cristian Freire, Manuel Pineda
Nivel de confidencialidad:	PÚBLICO

Historial de versiones:

Fecha	Versión	Creado por:	Descripción de la modificación
04/06/2014	1.0	**CONSEJO DE LA JUDICATURA** David Moncayo	Creación del documento.
17/10/2014	2.0	**CONSEJO DE LA JUDICATURA** David Moncayo Flor Chancay	Se realizó actualización de la documentación presentada ante SENATEL para obtener acreditación.
08/09/2016	3.0	**CONSEJO DE LA JUDICATURA** David Moncayo Flor Chancay	Se introduce cambios según Acuerdo Ministerial No. 012-2016 de 23 de mayo de 2016. Se realizó actualización de roles y puntos relacionados con renovación de certificados.
08/12/2017	4.0	**CONSEJO DE LA JUDICATURA** Jorge Navarrete Flor Chancay	Se incorporó texto relacionado con la existencia del Plan de Continuidad del Negocio.
14/05/2024	5.0	**CONSEJO DE LA JUDICATURA** Cristian Freire Manuel Pineda	Se realizó la actualización respecto a la normativa vigente previa a la renovación de la acreditación de la entidad de certificación.

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 y para el público en general, 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 del Consejo de la Judicatura como Entidad de Certificación de Información y Servicios Relacionados.

La Entidad de Certificación del Consejo de la Judicatura es una Entidad de Certificación de Información y Servicios Relacionados inscrita en el Registro Público Nacional de Entidades de Certificación de Información y Servicios Relacionados Acreditadas y Terceros Vinculados a cargo de la Secretaría Nacional de Telecomunicaciones para brindar los servicios de certificación digital.

Actualmente la **Agencia de Regulación y Control de las Telecomunicaciones** (ARCOTEL) nace adscrita al Mintel a partir del año 2015, como resultado de la Ley Orgánica de Telecomunicaciones y fusionando a las entidades Superintendencia de Telecomunicaciones (SUPERTEL), a la Secretaría Nacional de Telecomunicaciones (SENATEL) y al Consejo Nacional de Telecomunicaciones (CONATEL). Esta entidad se encarga de la administración, regulación y control de las telecomunicaciones y del espectro radioeléctrico como su gestión, así como de los aspectos técnicos de la gestión de medios de comunicación social que usen frecuencias del espectro radioeléctrico o que instalen y operen redes.

Según decreto ejecutivo de gobierno 1356 en su artículo 4 determina que: *"(...) la acreditación como entidad de certificación de información y Servicios relacionados comprende el derecho para la instalación, modificación, ampliación y operación de la infraestructura requerida para tal fin y estará sujeta al pago de valores, los que serán fijados por el CONATEL. (...)".*

Considerar la condición de la entidad ARCOTEL, señalada en el párrafo anterior que, mediante fusión gubernamental de entidades, reemplaza a la antecesora CONATEL.

En relación al acuerdo ministerial 1356 según decreto ejecutivo de gobierno, en su artículo 4. señala *"(…) El plazo de duración de la acreditación será de 10 años renovables por igual período, previa solicitud escrita presentada a la Secretaría de Telecomunicaciones con tres meses de anticipación al vencimiento del plazo. Siempre y cuando la Entidad de Certificación de Información haya cumplido con sus obligaciones legales y reglamentarias, así como las que conste en la resolución de acreditación. (…)".* Dichas obligaciones se encuentran disponibles en la página web oficial de la entidad ARCOTEL en el enlace https://www.arcotel.gob.ec/requisitos-entidades-de-certificacion/.

El área de firma electrónica dio a conocer a la Dirección de Tecnologías, la necesidad de esta acción técnica, en razón de las atribuciones y responsabilidades normativas según "ESTATUTO ORGÁNICO DE GESTIÓN POR PROCESOS DEL CONSEJO DE LA JUDICATURA" emitido desde el año 2014 y el vigente actualmente al 2024, el cual contiene cumplimientos necesarios según atribuciones y responsabilidades.

En cumplimiento de la norma institucional previamente citada, así como las determinadas por la entidad de regulación, fue remitido el Memorando circular CJ-DNTICS-SNS-2024-0007-MC de asunto **"INFORME DE NECESIDAD PARA LA**

RENOVACIÓN DE LA ACREDITACIÓN DE ENTIDAD DE CERTIFICACIÓN DE FIRMA ELECTRÓNICA", con su respectivo **análisis.**

En respuesta, la Dirección General mediante memorando CJ-DG-2024-0872-MC Iniciar Proceso De Renovación, dispone:

"(...) Sobre la base de lo expuesto, dispongo a la Dirección Nacional de Tecnologías de la Información y Comunicaciones a su cargo, en coordinación con las áreas pertinentes, ***iniciar el proceso para la renovación de la acreditación del Consejo de la Judicatura como Entidad de Certificación de Firma Electrónica****.* De las acciones realizadas se mantendrá informado a este despacho. *(...)".*

1.1. Presentación general del documento

El presente documento establece los lineamientos a seguir por parte de la Entidad de Certificación del Consejo de la Judicatura ICERT-EC para la prestación de Servicios de Información y Servicios Relacionados que incluye la emisión de certificados digitales de firma electrónica, sellado electrónico de tiempo y servicios relacionados.

En el documento se detallan las prácticas a seguir en la aprobación, emisión, gestión de certificados (incluyendo publicación y archivo), revocación, renovación, suspensión, reactivación y demás prácticas del ciclo de vida del certificado.

Esta Declaración de Prácticas de Certificación recoge las normas que se emplean dentro de la Entidad de Certificación de Información y Servicios Relacionados vinculadas al ciclo de vida de los certificados digitales y los controles para garantizar el servicio.

Los certificados que se emiten son los siguientes:

- **Certificado de Persona Natural**
  - Certificados en dispositivo criptográfico de tipo HW-token/tarjeta.
  - Certificados en dispositivo criptográfico de tipo hardware HSM SFC.
  - Certificados en archivo SW-PKCS #12.
- **Certificados de Persona Jurídica Privada**
  - Certificado en dispositivo criptográfico de tipo HW-token/tarjeta.
  - Certificados en dispositivo criptográfico de tipo hardware HSM SFC.
  - Certificado en archivo SW-PKCS#12.
- **Certificado de Miembro de Empresa**
  - Certificado en dispositivo criptográfico de tipo HW-token/tarjeta.

  - Certificados en dispositivo criptográfico de tipo hardware HSM SFC.
  - Certificado en archivo SW-PKCS#12.
- **Certificados de Empresa o Institución**
  - Certificado en hardware dispositivo criptográfico de tipo HW-HSM SFC.
  - Certificado en archivo SW-PKCS#12.
- **Certificados de departamento de empresa o institución**
  - Certificados en archivo SW-PKCS #12.
  - Certificado en Hardware Dispositivo criptográfico de tipo HW-HSM SFC.
- **Certificados de sellado de tiempo**

1.2. Nombre del documento e identificación

Este documento se denomina Declaración de Prácticas de Certificación, el cual contiene la siguiente información que podrá ser consultada en la página web de la ICERT-EC www.icert.fje.gob.ec.

Nombre del documento	*DECLARACIÓN DE PRÁCTICAS DE CERTICACIÓN DE LA ENTIDAD DE CERTIFICACIÓN DEL CONSEJO DE LA JUDICATURA ICERT-EC*
Identificador OID	*1.3.6.1.4.1.43745.1.1*
Versión	*4.0*
Fecha de emisión	*10 de mayo de 2024*
Ubicación URL	http://www.icert.fje.gob.ec/dpc/declaracion_practicas_certificacion.pdf

1.2.1. Identificadores de certificados

Número OID	Tipo de Certificados
1.3.6.1.4.1.43745.1.2.1.1	**Certificado de Persona Natural**
1.3.6.1.4.1.43745.1.2.1.1.1	Certificado de Persona Natural - Hardware
1.3.6.1.4.1.43745.1.2.1.1.1.1	Certificado de Persona Natural - Hardware - Token/Tarjeta
1.3.6.1.4.1.43745.1.2.1.1.1.2	Certificado de Persona Natural - Hardware - HSM SFC
1.3.6.1.4.1.43745.1.2.1.1.1.3	Certificado de Persona Natural - Hardware - HSM
1.3.6.1.4.1.43745.1.2.1.1.2	Certificado de Persona Natural - Software
1.3.6.1.4.1.43745.1.2.1.1.2.1	Certificado de Persona Natural - Software - Archivo (PKCS #12)

Número OID	Tipo de Certificados
1.3.6.1.4.1.43745.1.2.1.2	**Certificados de Persona Jurídica Privada**
1.3.6.1.4.1.43745.1.2.1.2.1	Certificados de Persona Jurídica Privada - Hardware
1.3.6.1.4.1.43745.1.2.1.2.1.1	Certificados de Persona Jurídica Privada - Hardware - Token/Tarjeta
1.3.6.1.4.1.43745.1.2.1.2.1.2	Certificados de Persona Jurídica Privada - Hardware - HSM SFC
1.3.6.1.4.1.43745.1.2.1.2.2	Certificados de Persona Jurídica Privada - Software
1.3.6.1.4.1.43745.1.2.1.2.2.1	Certificados de Persona Jurídica Privada - Software - Archivo (PKCS#12)

Número OID	Tipo de Certificados
1.3.6.1.4.1.43745.1.2.1.4	**Certificado de Miembro de Empresa**
1.3.6.1.4.1.43745.1.2.1.4.1	Certificado de Miembro de Empresa - Hardware
1.3.6.1.4.1.43745.1.2.1.4.1.1	Certificado de Miembro de Empresa - Hardware - Token/Tarjeta
1.3.6.1.4.1.43745.1.2.1.4.1.2	Certificado de Miembro de Empresa - Hardware - HSM SFC
1.3.6.1.4.1.43745.1.2.1.4.1.3	Certificado de Miembro de Empresa - Hardware - HSM
1.3.6.1.4.1.43745.1.2.1.4.2	Certificado de Miembro de Empresa - Software
1.3.6.1.4.1.43745.1.2.1.4.2.1	Certificado de Miembro de Empresa - Software - Archivo (PKCS #12)

Número OID	Tipo de Certificados
1.3.6.1.4.1.43745.1.2.2.1	**Certificado - Empresa o Institución**
1.3.6.1.4.1.43745.1.2.2.1.1	Certificado - Empresa o Institución – Hardware
1.3.6.1.4.1.43745.1.2.2.1.1.2	Certificado - Empresa o Institución - Hardware - HSM Remoto SFC
1.3.6.1.4.1.43745.1.2.2.1.2	Certificado - Empresa o Institución - Software
1.3.6.1.4.1.43745.1.2.2.1.2.1	Certificado de Empresa o Institución - Hardware - HSM

Número OID	Tipo de Certificados
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)

Número OID	Tipo de Certificados
1.3.6.1.4.1.43745.2.1	**DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN SELLADO DE TIEMPO**

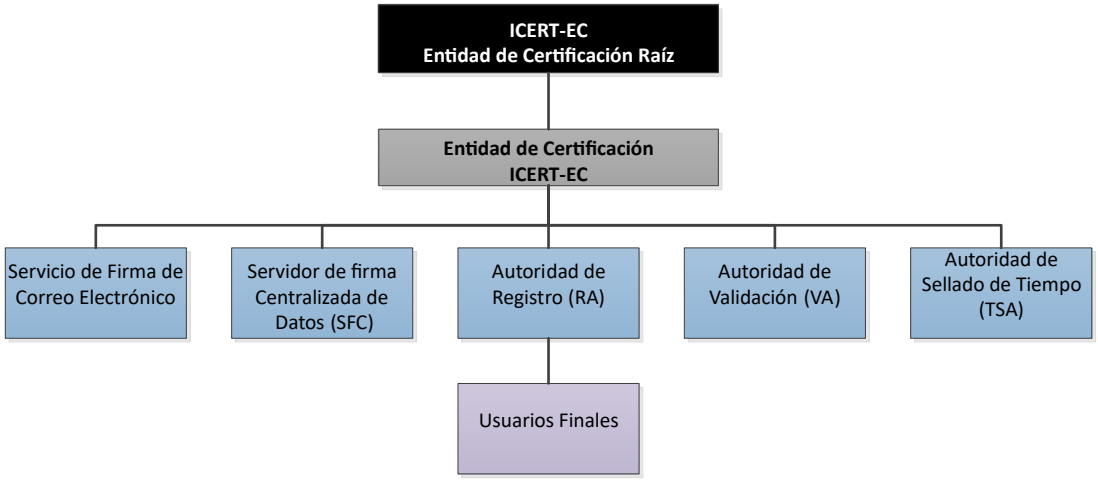
1.3. Participantes de la PKI

Los participantes de la PKI que forman la Entidad de Certificación del Consejo de la Judicatura son:

- Autoridad de Certificación (CA) Raíz
- Autoridad de Certificación (CA) Subordinada
- Autoridades de Registro (RA)
- Autoridad de Validación (VA)
- Autoridad de Sellado de Tiempo (TSA)
- Suscriptores de certificados
- Terceros vinculados

En el futuro se podrán incorporar nuevos elementos a la infraestructura de clave pública, en función de las necesidades del Consejo de la Judicatura.

La estructura jerárquica de la Entidad de Certificación del Consejo de la Judicatura es la siguiente:



CA Raíz: Autoridad de Certificación de primer nivel, esta CA sólo emite certificados para sí misma y su(s) CA Subordinada(s).

Únicamente estará en funcionamiento durante la generación del certificado autofirmado; de certificados de CA Subordinada y periódicamente para la generación de la Lista de Certificados Revocados de Autoridad de Certificación Raíz ARL o LRA.

La CA Raíz también emite los certificados de CA Subordinada mediante el procesamiento de las correspondientes peticiones realizadas por operadores con un rol determinado.

CA Subordinada: Autoridad de Certificación Subordinada, su función es la emisión de certificados de usuario final de los siguientes tipos:

- Certificados de firma electrónica para personas (persona natural, persona jurídica de derecho público o privado, miembro de empresa), entidades y unidades organizativas.
- Certificados de Autoridad de Sellado de Tiempo TSA CJ.
- Certificados de Autoridad de Validación VA CJ OCSP.

El formato de los certificados emitidos por las CA Raíz y Subordinada es X.509 v3 conforme al estándar RFC 5280.

A continuación, se describen las siguientes especificaciones para cada una de las entidades participantes:

1.3.1. Autoridades de Certificación (Certification Authority en idioma inglés, CA en siglas)

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

Los datos del certificado de la CA Raíz son los siguientes:

Nombre distintivo	CN	*ICERT-EC ENTIDAD DE CERTIFICACION RAÍZ*
	OU	*SUBDIRECCION NACIONAL DE SEGURIDAD DE LA INFORMACION DNTICS*
	O	*CONSEJO DE LA JUDICATURA*
	L	*DM QUITO*
	C	*EC*
Número de serie	72 57 0f 97 50 96 51 a6	
Nombre distintivo del emisor	CN	*ICERT-EC ENTIDAD DE CERTIFICACION RAIZ*
	OU	*SUBDIRECCION NACIONAL DE SEGURIDAD DE LA INFORMACION DNTICS*
	O	*CONSEJO DE LA JUDICATURA*
	L	*DM QUITO*
	C	*EC*
Período de validez	jue 2014 12:40:13	
	2034 12:40:13	

Los datos del certificado de la CA Subordinada son los siguientes:

	CN	*ENTIDAD DE CERTIFICACION ICERT-EC*

Nombre distintivo	OU	*SUBDIRECCION NACIONAL DE SEGURIDAD DE LA INFORMACION DNTICS*
	O	*CONSEJO DE LA JUDICATURA*
	L	*DM QUITO*
	C	*EC*
Número de serie	55 31 d3 80 ce 67 a9 54	
Nombre distintivo del emisor	CN	*ICERT-EC ENTIDAD DE CERTIFICACION RAIZ*
	OU	*SUBDIRECCION NACIONAL DE SEGURIDAD DE LA INFORMACION DNTICS*
	O	*CONSEJO DE LA JUDICATURA*
	L	*DM QUITO*
	C	*EC*
Período de validez	2014 13:34:52	
	2034 13:34:52	

1.3.2. Autoridad de Registro (Registration Authority en idioma inglés, RA en siglas)

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

Está facultada además para solicitar a la CA Subordinada la revocación, suspensión, y reactivación de certificados.

En la Entidad de Certificación del Consejo de la Judicatura, la Autoridad de Registro es la encargada de validar la identidad de los solicitantes y mediante procesos certificados y autenticados procesar las solicitudes respectivas. Los tipos de certificados que emite Entidad de Certificación del Consejo de la Judicatura serán para uso de cualquier persona natural o jurídica interesada.

La Autoridad de Registro llevará un registro completo de los solicitantes que ingresen una solicitud para obtener un certificado.

1.3.3. Autoridad de Validación (Validation Authority en idioma inglés, VA en siglas)

La Autoridad de Validación proporciona el servicio para la validación de los certificados de entidad final emitidos por la CA Subordinada a través del protocolo de consulta en línea de estado de certificados OCSP conforme al estándar RFC 2560.

Las respuestas OCSP están firmadas con la clave privada correspondiente al certificado de firma de respuestas OCSP de la Autoridad de Validación emitido por la Entidad de Certificación del Consejo de la Judicatura.

1.3.4. Autoridad de Sellado de Tiempo (Timestamping Authority en idioma inglés, TSA en siglas)

La Autoridad de Sellado de Tiempo proporciona el servicio de emisión de tokens de sellado de tiempo (TST), que indica que una firma, certificado o dato ha existido y no ha sido alterado desde un instante específico en el tiempo, a través del protocolo TSP conforme al estándar RFC 3161.

La sincronización de la hora de los equipos de la TSA de los entornos de producción, contingencia y pruebas se la realiza mediante el protocolo de sincronización de tiempo en red NTP ofrecido por el Instituto Oceanográfico de la Armada INOCAR hora oficial de Ecuador.

Los sellos de tiempo emitidos están firmados con la clave privada correspondiente al certificado de firma de sellos de tiempo de la AST emitido por la Entidad de Certificación del Consejo de la Judicatura.

1.3.5. Servicio de Firma de Correo Electrónico

Los usuarios con certificados digitales almacenados remotamente podrán firmar los correos electrónicos enviados directamente desde el cliente de correo electrónico instalado en su computadora, a través del software seguro desarrollado para tal propósito.

1.3.6. Servidores de Firma Centralizada (SFC) de datos

Los Servidores de Firma Centralizada de datos almacenan certificados que permiten realizar operaciones de firma electrónica mediante la gestión centralizada de las claves y los certificados de firma de entidad final.

El SFC de datos permite a los usuarios utilizar sus claves y certificados para realizar firmas electrónicas.

1.3.7. Usuarios finales

Los suscriptores son usuarios finales, personas físicas o jurídicas que tienen capacidad para solicitar y obtener un certificado digital bajo las premisas establecidas en la presente Declaración de Prácticas de Certificación y las políticas de certificado vigentes para cada tipo de certificado. Son usuarios finales: solicitantes, suscriptores y terceros que confían en certificados emitidos por la Entidad de Certificación del Consejo de la Judicatura.

1.3.7.1. Solicitante

El solicitante es aquella persona natural o jurídica, que a nombre propio o con representación legal de la empresa o entidad, desea acceder a los servicios de certificación digital y previa identificación solicita la emisión de un certificado digital a Entidad de Certificación del Consejo de la Judicatura.

Cuando se trata de una persona jurídica el solicitante solamente puede ser el representante legal o administrador de la entidad jurídica suscriptora del certificado.

1.3.7.2. Suscriptor

El suscriptor es aquella persona natural o jurídica a quien se le otorga un certificado digital emitido por la Entidad de Certificación del Consejo de la Judicatura y se considera suscriptor mientras dicho certificado se encuentre vigente. Suscriptores son aquellas personas que poseen y gestionan actividades mediante el uso de un certificado digital. El suscriptor es el titular del certificado cuya identidad es única e irrevocablemente la registrada en la creación del certificado y la persona que asume la responsabilidad de la firma de los documentos digitales.

1.3.7.3. Terceros vinculados

Los terceros vinculados son las personas o entidades ajenas a la Entidad de Certificación del Consejo de la Judicatura que en forma libre y voluntaria deciden confiar y aceptar un certificado digital emitido por la ICERT-EC.

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.

1.4. Uso de los certificados

1.4.1. Uso apropiado de los certificados

Los certificados de diferentes tipos emitidos por las CA Raíz y Subordinada bajo esta DPC serán utilizados solamente durante su período de vigencia para dar cumplimiento a las funciones que le son propias y legítimas.

Los certificados deben utilizarse de acuerdo con los fines y especificaciones definidos en las respectivas políticas de certificados y solamente pueden ser utilizados para los fines contemplados en las Prácticas de Certificación.

1.4.1.1. Certificado de persona natural o física

El certificado de persona natural o física 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:

1.4.1.1.1. Autenticación de identidad

El certificado puede utilizarse para identificar a una persona natural ante servicios y aplicaciones informáticas, confirmando su autenticidad e integridad.

1.4.1.1.2. Firma digital

Las firmas digitales efectuadas con certificados de persona natural ofrecen los medios de respaldo al garantizar la autenticidad del origen, la integridad de los datos firmados y el no repudio.

1.4.1.1.3. 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.

1.4.1.1.4. Integridad del documento

La utilización del certificado garantiza que el documento es íntegro, 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.

1.4.1.1.5. 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 permite demostrar la identidad del emisor sin que este pueda repudiarlo.

1.4.1.2. Certificado de persona jurídica privada

El certificado de persona jurídica privada 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:

1.4.1.2.1. Autenticación de identidad

El certificado puede utilizarse para identificar a una persona jurídica privada ante servicios y aplicaciones informáticas, confirmando su autenticidad e integridad.

1.4.1.2.2. Firma digital

Las firmas digitales efectuadas con certificados de persona jurídica privada ofrecen los medios de respaldo al garantizar la autenticidad del origen, la integridad de los datos firmados y el no repudio.

1.4.1.2.3. 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.

1.4.1.2.4. 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.

1.4.1.2.5. 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 permite demostrar la identidad del emisor sin que este pueda repudiarlo.

1.4.1.3. Certificado de miembro de empresa

El certificado de miembro de empresa 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:

1.4.1.3.1. Autenticación de identidad

El certificado puede utilizarse para identificar a una persona física en su calidad de miembro de empresa ante servicios y aplicaciones informáticas, confirmando su autenticidad e integridad.

1.4.1.3.2. Firma digital

Las firmas digitales efectuadas con certificados de miembro de empresa ofrecen los medios de respaldo al garantizar la autenticidad del origen, la integridad de los datos firmados y el no repudio.

1.4.1.3.3. 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.

1.4.1.3.4. 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.

1.4.1.3.5. 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 permite demostrar la identidad del emisor sin que este pueda repudiarlo.

1.4.1.4. Certificado de empresa o institución

El certificado 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:

1.4.1.4.1. Autenticación de identidad

El certificado puede utilizarse para identificar a una empresa o institución ante servicios y aplicaciones informáticas, confirmando su autenticidad e integridad.

1.4.1.4.2. Firma digital

Las firmas digitales efectuadas con certificados 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.

1.4.1.4.3. 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.

1.4.1.4.4. 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.

1.4.1.4.5. 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 permite demostrar la identidad del emisor sin que este pueda repudiarlo.

1.4.1.5. Certificado de departamento de empresa o institución

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:

1.4.1.5.1. 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.

1.4.1.5.2. 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.

1.4.1.5.3. 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.

1.4.1.5.4. 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.

1.4.1.5.5. 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.

1.4.1.6. Certificado de sellado de tiempo

La prestación del servicio de sellado de tiempo se realiza en base a la RFC3161 *"HTTP Time-Stamp Protocol via HTTP".* El servicio toma al momento temporal de su reloj interno, sincronizado con la hora oficial del Ecuador (INOCAR) y genera una marca temporal. Esta marca temporal viene firmada por el certificado de la TSA, lo cual le otorga garantías de autenticidad e integridad.

La Autoridad de Sellado de Tiempo se comunica con la base de datos donde se almacenan los datos sobre los sellos de tiempo emitidos y con una fuente fiable de tiempo en red NTP para sincronizar la hora a intervalos regulares.

Realizar los controles de seguridad y procedimientos operacionales necesarios para prevenir amenazas a las inversiones y negocios.

Los sellos de tiempo emitidos están firmados con la clave privada correspondiente al certificado de firma de sellos de tiempo de la TSA.

1.4.2. Usos prohibidos de los certificados

La realización de operaciones no autorizadas según esta DPC, 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 de los certificados de usuario final para firmar otros certificados o listas de revocación (CRL).
- Está prohibido utilizar los certificados para usos distintos a los estipulados en los numerales correspondientes a: 1.4.1 *Uso apropiado de los certificados y 1.4.2 Usos prohibidos de los certificados.*
- No están permitidas alteraciones sobre los certificados emitidos por la Entidad de Certificación del Consejo de la Judicatura ICERT-EC.

- Se prohíbe el uso de certificados que puedan ocasionar daños personales o medioambientales.
- Se prohíbe toda acción que infrinja las disposiciones, obligaciones y requisitos estipulados en la presente DPC.
- 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.
- ICERT-EC no está autorizada para 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.

1.5. Administración de la Declaración de Prácticas de Certificación

La Subdirección Nacional de Seguridad de la Información es la instancia que administra la presente Declaración de Prácticas de Certificación, encargada también de la elaboración, registro, mantenimiento y actualización de la DPC y las PC.

Los datos de la Entidad de Certificación y de la persona de contacto disponibles para información al respecto son:

1.5.1. Organización que administra la DPC

ENTIDAD DE CERTIFICACIÓN	*Entidad de Certificación Consejo de la Judicatura ICERT – EC*
NOMBRE	*Subdirección Nacional de Seguridad de la Información DNTICs*
DIRECCIÓN	*Av. 12 de Octubre N24-563 y Francisco Salazar*
TELÉFONO	*(02) 395 3600*
e- mail	entidad.certificacion@funcionjudicial.gob.ec

1.5.2. Persona de contacto

ENTIDAD DE	*Entidad de Certificación Consejo de la Judicatura ICERT – EC*

CERTIFICACIÓN	
NOMBRE	*Ing. Peter Cabrera* *Subdirector Nacional de Seguridad de la Información*
DIRECCIÓN	*Av. 12 de Octubre N24-563 y Francisco Salazar*
TELÉFONO	*(02) 395 3600*
e- mail	entidad.certificacion@.funcionjudicial.gob.ec

1.5.3. Persona que determina la idoneidad e integridad de la DPC

La persona que determina la idoneidad e integridad de la DPC es el titular de la Subdirección Nacional de Seguridad de la Información.

1.5.4. Procedimientos de aprobación de la DPC

La Declaración de Prácticas de Certificación es administrada por la Subdirección Nacional de Seguridad de la Información del Consejo de la Judicatura y aprobada por el Consejo de la Judicatura.

1.6. Definiciones y siglas

1.6.1. Definiciones

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

Antivirus: Programas informáticos cuyo objetivo es detectar y eliminar virus informáticos.

Ataques DDoS: Ataque de denegación de servicio que causa que un servicio informático sea inaccesible a los usuarios legítimos del sistema.

Ataques MitM: Ataque informático por el cual un usuario no autorizado adquiere la capacidad de leer, insertar y modificar datos en tránsito de un servicio informático.

Ataque de Inyección SQL: Ataques orientados a realizar consultas no autorizadas en las Bases de datos de los sistemas informáticos.

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 (Certification Authentication en idioma inglés, CA en siglas): Entidad encargada de emitir y revocar certificados digitales utilizados en firma electrónica y cuya clave pública está incluida en el.

Autoridad de Registro (Registration Authority en idioma inglés, RA en siglas): 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 sus certificados.

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

Balanceador de carga: Hardware o software utilizado para la administración de sistemas informáticos cuyo principio es distribuir el trabajo entre varios servidores, procesos, discos u otros recursos informáticos.

CRL (Certificate Revocation List en idioma inglés): 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 CA, 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 de la Entidad de Certificación del Consejo de la Judicatura existen la Autoridad de Certificación Raíz y la Autoridad de Certificación Subordinada.

Datos personales: Se define como un dato que identifica o hace identificable a una persona natural directa o indirectamente según la Ley Orgánica de Protección de Datos Personales.

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, en idioma inglés): Es un componente o dispositivo criptográfico utilizado para generar, almacenar y proteger claves criptográficas.

OCSP (Online Certificate Status Protocol, en idioma inglés): 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, en idioma inglés): 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, en idioma inglés): 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, en idioma inglés): 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, en idioma inglés): 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)*.

Suscriptor: Persona o entidad que solicita los servicios proporcionados por la Autoridad de Certificación ICERT-EC.

WAF: (Firewall de aplicaciones web): Un firewall de aplicaciones web es un tipo de firewall que supervisa, filtra o bloquea el tráfico HTTP hacia y desde una aplicación web.

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.

1.6.2. Siglas

Siglas	Palabras abreviadas
ASCII	American Standard Code for Information Interchange
ARL	Authority Revocation List (Lista de revocación de autoridad)
API	Application Programming Interface (Interfaz de Programación de Aplicaciones)
BD	Base de Datos
VA	Validation Authority (Autoridad de Validación)

C	Country Name (Nombre del País)
CA	Certification Authority (Autoridad de Certificación)
CAdES	CMS Advanced Electronic Signatures
CAdES-XL	CMS Advanced Electronic Signatures eXtended Long-term
CJ	Consejo de la Judicatura
CN	Common Name (Nombre común)
cps	certificate practice statement
CRL	Certificate Revocation List (Lista de certificados revocados)
CSP	Cryptographic Service Provider
DD	Day Day
DN	Distinguished Name (Nombre distintivo)
DPC	Declaración de Prácticas de Certificación
DNS	Domain Name System
DNTICs	Dirección Nacional de Tecnologías de la Información y Comunicaciones
EAL4+	Evaluation Assurance Level 4+
ERC	Emergency Revocation Code (Código de revocación emergente)
FC	Firma Centralizada
FIFO	First Input First Output
FIPS	Federal Information Processing Standards
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 (Protocolo Internet)
ISO	International Organization for Standardization (Organismo internacional de estandarización)
L	LocalityName
MM	Month Month
mm	Minute minute
NIST	National Institute of Standards and Technology
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	Organizational UnitName
PAdES	PDF Advanced Electronic Signature
PAdES-LTV	PAdES Long Term Validation
PC	Política de Certificados
PDF	Portable Document Format
PDF/A	PDF/Archive
PIN	Personal Identification Number (Número de identificación personal)
PKCS	Public-Key Cryptography Standard (Estándares de criptografía de clave pública)
PKI	Public Key Infrastructure (Infraestructura de Clave Pública)
PUK	Personal Unlok Key (Clave personal de desbloqueo)
RA	Registration Authority (Autoridad de registro)
RFC	Request For Comments (Petición de comentarios)
RSA	Rivest Shamir Adleman
RUC	Registro Único de Contribuyentes
SFC	Servidor de Firma Centralizada
SHA	Secure Hash Algorithm
SMTP	Simple Mail Transfer Protocol
SW	Software
ss	second second
TSP	Time-Stamp Protocol (Protocolo de estampado de tiempo)
URL	Uniform Resource Locator
UTC	Universal Time Coordinated
UTF-8	8-bit Unicode Transformation Format
v	version
VA	Validation Authority (Autoridad de validación)
XADES	XML Advanced Electronic Signatures
XADES-XL	XML Advanced Electronic Signatures eXtended Long-term
YYYY	Year Year Year Year

2. Publicación de la información y responsabilidad de los repositorios

La responsabilidad de la publicación de la presente DPC, de los documentos de políticas de certificados, así como la lista de los certificados emitidos, el estatus de estos y las CRL, le corresponde a la Subdirección Nacional de Seguridad de la Información del Consejo de la Judicatura. La Declaración de Prácticas de Certificación y las políticas de certificado son documentos públicos que se encuentran disponibles en la página web de la Entidad de Certificación del Consejo de la Judicatura. Las modificaciones a los documentos mencionados que fueren aprobadas de acuerdo con el procedimiento establecido se harán públicas de forma inmediata.

2.1. Repositorios

La documentación mencionada en el párrafo anterior se encuentra disponible en la página web de la Entidad de Certificación del Consejo de la Judicatura. La Declaración de Prácticas de Certificación (DPC) de 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, estará disponible para suscriptores y usuarios que podrán consultar en el repositorio de documentos vía electrónica, expuesto en la página web.

Garantizando la disponibilidad permanente de la información, disponemos de un servidor duplicado y balanceado, de manera que, en caso de falla de su principal, la información estará disponible.

2.2. Publicación de la DPC

La Declaración de Prácticas de Certificación estará disponible a través de: http://www.icert.fje.gob.ec/dpc/declaracion_practicas_certificacion.pdf.
Cualquier cambio o modificación en la DPC de la Entidad de Certificación del Consejo de la Judicatura 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 los documentos.

2.3. Frecuencia de la publicación

Cada vez que se produzca un cambio o modificación en los documentos de prácticas y políticas de certificados siguiendo el procedimiento establecido en la sección 9.12 de este documento se realiza la correspondiente publicación.

Una vez que han sido emitidos por la CA Subordinada los certificados de entidad final, éstos serán publicados automáticamente por la RA en los repositorios establecidos. El directorio de certificados se actualiza en forma permanente para dar a conocer los certificados que se encuentran vigentes.

2.4. Control de acceso a los repositorios

El acceso a la consulta del directorio de certificados, el estatus de los certificados y la CRL es libre, no obstante, al igual que en todos los procesos de la vida de los certificados la ICERT-EC dispone de la seguridad y controles para garantizar que la información del directorio no sea alterada.

Es responsabilidad de la Entidad de Certificación establecer controles que impidan a personas no autorizadas manipular la información contenida en los repositorios, así como la adopción de las medidas de seguridad necesarias para precautelar 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 (RA) y la Autoridad de Certificación (CA) en el momento de autenticar la identidad del solicitante y aprobar la emisión de un certificado.

Previo a la emisión inicial de un certificado digital, el solicitante deberá realizar a su responsabilidad, el ingreso de datos necesarios para la emisión del certificado a través de un formulario de registro ubicado en el sitio web de la Entidad de Certificación del Consejo de la Judicatura.

Las Autoridades de Registro de la ICERT-EC realizarán el mismo procedimiento para identificar y registrar a un suscriptor de certificados, de modo tal de ofrecer un grado de confianza equivalente para cualquier suscriptor de un certificado emitido por la CA.

En el caso de una persona natural con nacionalidad ecuatoriana, el nombre debe estar conformado por nombres y apellidos tal como consta en la cedula de ciudadanía. Si la persona natural es un extranjero, el nombre debe estar conformado por nombres y apellidos tal como consta en el pasaporte o documento equivalente.

En el caso de una persona jurídica el nombre que constará en el certificado corresponde a la razón social que conste en el RUC, **no se admitirá nombres abreviados.**

3.1. Acerca de los nombres

De acuerdo con la 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.

3.1.1. Tipos de nombres

Los titulares de certificados emitidos por ICERT-EC requieren la plena identificación del suscriptor mediante un nombre distintivo (Distinguished Name) de acuerdo con el estándar X.500.

Los nombres contenidos en los certificados son los siguientes:

3.1.1.1. Certificado de persona natural o física

Todos los certificados de persona natural 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.

Abreviatura	Nombre	Descripción
C	País	*Abreviatura del país donde reside el suscriptor*
L	Ciudad	*Ciudad donde reside el suscriptor*
SerialNumber	Número Serial	*Número del documento de identificación de la persona natural*
CN	Nombre común	*Nombres y apellidos completos del suscriptor*

3.1.1.2. Certificado de persona jurídica privada

Todos los certificados de persona jurídica privada 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.

Abreviatura	Nombre	Descripción
C	País	*Abreviatura del país donde reside el suscriptor*
O	Razón social	*Razón social de la empresa*
L	Ciudad	*Ciudad de la empresa*
SerialNumber	Número Serial	*Número de cédula o pasaporte del representante legal de la persona jurídica privada*
CN	Nombre común	*Nombres y apellidos del representante legal de la persona jurídica privada*

3.1.1.3. Certificado de miembro de empresa

Todos los certificados de miembro de empresa 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 de miembro de empresa*
CN	Nombre común	*Nombres y apellidos completos del suscriptor*

3.1.1.4. Certificado de empresa o institución

Todos los certificados 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	*Ciudad donde reside el suscriptor*
SerialNumber	Número Serial	*RUC de la empresa o institución*
CN	Nombre común	*Razón social de la empresa o institución*

3.1.1.5. Certificado de departamento de empresa o institución

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	*Ciudad donde reside el suscriptor*
SerialNumber	Número Serial	*Número del documento identificación del representante legal*
CN	Nombre común	*Nombres y apellidos completos del suscriptor*

3.1.1.6. Certificado de pruebas o test

Para los ambientes de test, desarrollo o pruebas de funcionamiento de la PKI se utilizarán nombres ficticios que denoten expresamente la invalidez de los certificados; por ejemplo, se utilizarán las palabras: “Test_Organización”, “Pruebas_Apellido”, “Prueba_Nombre” entre otros que denoten la invalidez legal y, por tanto; sin responsabilidad alguna sobre ICERT-EC. Se realiza la emisión de estos certificados únicamente para realizar pruebas de funcionamiento,

pruebas de contingencia y/o auditorías por parte del ente de control para evaluación técnica.

3.1.2. Necesidad de que los nombres sean significativos

Todo certificado 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.

3.1.3. Anónimos y seudónimos en los nombres

La ICERT-EC no admite anónimos ni seudónimos para identificar el nombre de una persona natural o jurídica, o para vincular o identificar los datos de un certificado con una persona natural.

3.1.4. Reglas para interpretar las diversas formas de nombres

La regla utilizada para interpretar los nombres de los titulares de certificados que emite la ICERT-EC es ISO/IEC 9594 (X.500).

3.1.5. Unicidad de los nombres

El nombre distintivo de los certificados será único para cada suscriptor y está relacionado con el identificador de usuario, sea éste una persona, dispositivo, entidad o unidad organizativa.

3.1.6. Reconocimiento, autenticación y marcas comerciales

La ICERT-EC no asume responsabilidad en la emisión de certificados que hagan uso de una marca comercial.

La ICERT-EC no estará obligada a determinar la propiedad intelectual y/o industrial de un nombre que aparece en una solicitud de certificado, sino que en principio se procederá con la emisión del certificado. Así mismo, se reserva el derecho de rechazar una solicitud de certificado debido a conflictos en nombres.

En caso de controversia o conflictos que se deriven de las políticas expresadas en este documento, se resolverá mediante los centros de mediación o arbitraje, que así lo determine la legislación ecuatoriana.

3.2. Validación inicial de la identidad

La ICERT-EC hará uso de mecanismos apropiados para validar la identidad del usuario cuando se solicite un certificado digital, así como el registro de la información del usuario, para lo cual verificará la identidad del solicitante.

3.2.1. Método para probar la posesión de la clave privada

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

a) Generación en token o tarjeta criptográfica

La RA permite al operador de emisión realizar la generación del par de claves de firma en el token o tarjeta criptográfica y del certificado emitido por la CA.

Completado dicho procedimiento, es posible descargar el certificado en formato PEM directamente desde el token/tarjeta inteligente.

Una vez finalizado el proceso, la RA envía al suscriptor el PIN del token/tarjeta criptográfica por correo electrónico. El PIN establecido es calculado a través de algoritmos y es 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 en HSM SFC y custodia segura remota

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

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

c) Generación y construcción de un PKCS#12 descargable

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

Una vez finalizado el proceso, la RA envía por correo electrónico al suscriptor la contraseña de acceso a su archivo PKCS#12. La contraseña establecida se calcula a través de algoritmos y es completamente desconocida para terceras partes.

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

d) Firma de una petición CSR PKCS#10 generada por el cliente

La RA permite al operador de emisión realizar la generación de un certificado emitido por la CA. Este certificado se construye a raíz del envío de un CSR (PKCS#10) por el suscriptor, que es creado una vez generadas las claves por sus medios. La RA permite el envío por correo electrónico del certificado digital en formato PEM.

El suscriptor debe indicar los medios utilizados para la generación de las claves, pudiendo ser estas generadas a través de un software dedicado o a través de un HSM, token o tarjeta inteligente certificados FIPS 140-2 Level 3 y/o Common Criteria EAL4+.

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

3.2.2. Autenticación de la identidad de una organización o persona jurídica

Para aprobar la pertenencia a una organización o empresa se requerirá la presentación de la información requerida para registro de empresa o institución publicada en el sitio web de la entidad de certificación.

Se debe presentar una autorización firmada o una constancia de identificación corporativa o institucional.

Para el caso de una persona jurídica, el representante ha de proporcionar toda información de registro existente, incluyendo los datos relativos a la constitución y personería jurídica y a la vigencia de las facultades de representación del solicitante, así como las limitaciones a las que se circunscriben sus actuaciones.

El solicitante para demostrar su identidad debe proporcionar la siguiente información y documentación para adquirir el certificado de Persona Jurídica Privada, 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 (si no tiene queda en blanco)***

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 con los procedimientos internos definidos por la ICERT-EC.

3.2.3. Autenticación de la identidad de una persona natural

Al momento de solicitar un certificado el solicitante debe identificarse de manera inequívoca y poder demostrar cuál es realmente su identidad mediante la presentación de la cédula de ciudadanía o pasaporte y de ser el caso, su pertenencia a una determinada empresa u organización.

El solicitante, para demostrar su identidad, debe proporcionar la siguiente información para adquirir el certificado de persona natural, conforme a la normativa aplicable y al cuadro de identificadores de campo:

NUMERO IDENTIFICADOR	CAMPOS
3.1	*Cédula o pasaporte*
3.2	*Nombre(s)*
3.3	*Primer apellido*
3.4	*Segundo apellido (si no tiene no aparece dentro del certificado)*
3.7	*Dirección*
3.8	*Teléfono*
3.9	*Ciudad*
3.12	*País*
3.11	*RUC: (si no tiene no aparece dentro del certificado)*

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

3.2.4. Información del o la solicitante no verificada

En la solicitud del certificado el solicitante debe proporcionar documentos y datos personales que lo identifican absolutamente, toda la información solicitada es verificada aún si no hace parte de la información incluida en el certificado digital. ICERT-EC no incluye información no verificada en los certificados emitidos.

3.2.5. Validación de la autoridad

Para proceder a validar la pertinencia de solicitud de certificados por parte del responsable de una entidad/autoridad se debe verificar las facultades de que dispone para el uso de un certificado digital.

3.2.6. Criterios para la interoperación

La definición de los criterios para la interoperación con otras CA es función de la Subdirección Nacional de Seguridad de la Información del Consejo de la Judicatura.

La Entidad de Certificación del Consejo de la Judicatura precautelará y permitirá la autenticación, validación y firma electrónica con los certificados digitales emitidos por todas las entidades de certificación de información y servicios relacionados debidamente acreditadas ante la entidad de control.

3.3. Requisitos de identificación y autenticación para solicitar una nueva clave

3.3.1. Identificación y autenticación para solicitar una nueva clave

El proceso de identificación para solicitud de una nueva clave es el requerido para el proceso de solicitud inicial de un certificado y está definido en la política de certificados respectiva. Es posible también la identificación haciendo uso del certificado original que se desea renovar, siempre que no haya caducado ni se haya provocado su revocación.

3.3.2. Identificación y autenticación para renovación de la clave después de la revocación

El proceso de identificación de un solicitante para solicitar una nueva clave luego de la revocación de un certificado es el mismo que el requerido para el proceso de solicitud inicial de un certificado.

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 el código de emergencia asociado ERC. También puede ser procesada mediante solicitud expresada en un oficio firmado por el representante de la empresa o institución, una solicitud debidamente sustentada enviada por un tercero que represente al suscriptor o mediante una comparecencia física ante la Autoridad de Registro por la que el operador de certificados procederá a la revocación.

4. Requisitos operacionales para el ciclo de vida de los certificados

Las especificaciones contenidas en este acápite lo son sin perjuicio de las estipulaciones previstas en cada una de las políticas de certificados establecidas para los diferentes tipos de certificados.

4.1. Solicitud de certificado

El procedimiento para solicitud de un certificado digital se describe detalladamente en la correspondiente política de certificados, sin perjuicio de la información requerida obligatoriamente.

4.1.1. Proceso de registro y responsabilidades

El solicitante de un certificado digital debe llenar el correspondiente formulario con toda la información requerida. No toda la información requerida en el proceso de registro aparecerá en el certificado y será conservada de manera confidencial por la Autoridad de Certificación.

La ICERT-EC en función de sus actividades, precautelará 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.

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

4.1.2. Proceso de solicitud del certificado

En el proceso de solicitud del certificado el solicitante debe suministrar diversos datos que lo identifican plenamente. La información proporcionada en la solicitud del certificado digital es verificada por la Autoridad de Registro con la finalidad de determinar su autenticidad.

4.2. Procesamiento de las solicitudes

Las solicitudes de emisión de un certificado digital serán direccionadas por la Autoridad de Registro a la Autoridad de Certificación para la verificación y autenticación de los datos registrados en la solicitud.

4.2.1. Procesamiento de identificación y autenticación

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

Para estos efectos el solicitante autoriza y faculta expresamente a la ICERT-EC y a su Autoridad de Registro, verificar la información entregada 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 por el lapso de cinco (5) años.

4.2.2. Aprobación o rechazo de la solicitud de certificados

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

Serán rechazadas notificando la causa, las solicitudes que no cumplan con los requerimientos, información y documentación solicitados o que los antecedentes que presentan no sean concordantes. El rechazo de la solicitud no impide que el solicitante pueda nuevamente iniciar el proceso de solicitud del certificado.

4.3. Emisión de certificados

La emisión del certificado se produce el momento en que la Autoridad de Certificación de la ICERT-EC ha comprobado fehacientemente la validez de la

solicitud realizada. El mecanismo para realizar esta validación está descrito en la política de certificados correspondiente.
Cuando la CA emite un certificado de acuerdo con una solicitud de certificación válida, se envía una copia de la clave pública a la RA que emitió la solicitud.
Le corresponde a la RA notificar al suscriptor de un certificado cuando se ha producido la emisión del certificado. En todo momento el usuario suscriptor es el único que tiene acceso a la clave privada del certificado digital.
Un usuario podrá tener varios certificados en distintos contenedores emitidos bajo distintas políticas de certificado.
En todo lo demás, relativo a la emisión del certificado se sujetará a lo estipulado en la correspondiente política de certificados.

4.3.1. Acciones de la CA durante la emisión del certificado

Con la emisión del certificado por parte de la CA de la Entidad de Certificación del Consejo de la Judicatura se perfecciona la autorización definitiva de la solicitud realizada por parte de quien la suscribe.
Todos los certificados entrarán en vigencia desde el momento de su emisión.

4.3.2. Notificación al suscriptor por parte de la CA de la emisión del certificado

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

4.4. Aceptación del certificado

4.4.1. 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 y al presente documento.

La aceptación se podrá considerar si la CA no recibe ninguna notificación por parte del suscriptor dentro de las cuarenta y ocho (48) horas posteriores a la emisión del certificado. Un suscriptor puede enviar un mensaje de no aceptación del certificado en el que el mensaje incluye el motivo del rechazo y se identifican los motivos, o de ser el caso los campos en el certificado que son incorrectos o incompletos.

4.4.2. Publicación del certificado por la CA

Una vez que se ha producido la emisión del certificado, la clave pública del certificado es publicada en el correspondiente repositorio de Base de Datos de la RA.

4.4.3. Notificación de la emisión del certificado

La notificación de la emisión del certificado se da por parte de la CA a otras entidades, como la RA.

4.5. Par de claves y uso del certificado

4.5.1. 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. La clave privada es de uso exclusivo del suscriptor para los fines estipulados en esta Declaración de Prácticas de Certificación.

El suscriptor sólo podrá utilizar la clave privada y el certificado exclusivamente para los usos autorizados en la política de certificados correspondiente. 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 en la política de certificado, y sólo para la realización de funciones que requieran acreditar la identidad del titular.

Una vez que el certificado haya expirado o haya sido revocado la clave privada del suscriptor deja de operar.

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

Los terceros que confían en los servicios de certificación del Consejo de la Judicatura solo pueden depositar su confianza en los certificados de funciones que requieran acreditar la identidad del titular, de conformidad con lo establecido en el campo uso permitido del certificado *"keyUsage"* del certificado o en la presente Declaración de Prácticas de Certificación.

Los usuarios que confían en el servicio de certificación del Consejo de la Judicatura deben verificar el estado del certificado utilizando los mecanismos establecidos en esta Declaración de Prácticas de Certificación.

4.6. Renovación del certificado

La Autoridad de Certificación de la Entidad de Certificación del Consejo de la Judicatura ICERT-EC procesa solicitudes de renovación de certificados que estén en un período de tres (3) meses previos a su expiración. Si el suscriptor desea obtener un nuevo certificado debe solicitar la emisión de un nuevo certificado cuando el anterior haya caducado o durante el período de tres (3) meses previos a su expiración.

4.6.1. Razones para la renovación del certificado

La renovación del certificado se produce cuando éste va a expirar y el suscriptor desea continuar usando un certificado. Para esto el suscriptor deberá presentar una solicitud de renovación y realizar el mismo proceso utilizado para solicitar un certificado.

Sin perjuicio de lo señalado en el inciso anterior, la Autoridad de Registro del Consejo de la Judicatura, notificará al suscriptor con 3 meses, 2 meses, 1 mes, 2 semanas, 1 semana y 1 día de anticipación la próxima 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.

4.6.2. ¿Quién puede solicitar la renovación de los certificados?

El suscriptor puede solicitar la renovación de un certificado de usuario final previo a su expiración.

4.6.3. Procesamiento de las solicitudes de renovación

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

4.6.4. Notificación de la emisión del nuevo certificado

La notificación al suscriptor acerca de la emisión del nuevo certificado se realiza igual que cuando se emitió el certificado por primera ocasión.

4.6.5. Conducta que constituye la aceptación del certificado renovado

Se procede igual que lo descrito en el numeral 4.4.1

4.6.6. Publicación del nuevo certificado por la CA

Se procede igual que lo descrito en el numeral 4.4.2

4.6.7. Notificación de la emisión del certificado a terceros

Se procede igual que lo descrito en el numeral 4.4.3.

4.7. Renovación de certificados con cambio de clave

Todas las renovaciones de certificados, 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.

4.7.1. Circunstancias para la renovación de un certificado con cambio de clave

Estar en el periodo de renovación de un certificado digital de la política de certificados correspondiente.

4.8. Modificación de certificados

4.8.1. 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 se tratarán como una nueva emisión de certificados.

Se modifica un certificado cuando 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.

4.9. Revocación, suspensión y reactivación de certificados

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

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

La revocación de un certificado tiene como efecto principal la terminación inmediata y anticipada del periodo de validez del certificado. Este acto no afectará las obligaciones subyacentes creadas o comunicadas 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).

4.9.1. Circunstancias para la revocación

Los certificados emitidos por la Autoridad de Certificación de la Entidad de Certificación del Consejo de la Judicatura deben ser revocados por los siguientes motivos:

- Traslado de funciones.
- Cesación de funciones.
- Fallecimiento del titular del certificado.
- 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.
- 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.
- Por el cese en la actividad como prestador de servicios de certificación por parte del Consejo de la Judicatura.

De producirse el compromiso de la clave del certificado de la CA o cuando el certificado de una RA o CA superior en la jerarquía de confianza del certificado es revocado, se deberá revocar y reemitir todos los certificados que fueron firmados con la clave comprometida.

4.9.2. 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 expreso de acuerdo al incumplimiento de políticas, normas o determinaciones internas institucionales debidamente motivadas respecto de sanciones de diferente índole a petición de parte con el debido sustento documental.

4.9.3. 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 que debe ser dirigida a la RA, 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.

4.9.4. Plazo límite del tiempo de suspensión

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

A su vez puede extenderse por el tiempo que señalen las determinaciones internas institucionales debidamente motivadas respecto de sanciones de diferente índole, a petición de parte con el debido sustento documental, y guarda relación con lo referido en el numeral 4.9.2 del presente documento.

4.10. 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 (VA) mediante el protocolo OCSP.

Se debe considerar la responsabilidad que tiene el propietario del certificado en calidad de usuario y el principio de buen uso del mismo, bajo los parámetros expuestos respecto de la suspensión o sus estados de certificado; señalando que estos son de estricta responsabilidad y cumplimiento con las consideraciones legales que implique su mal uso o uso no autorizado de acuerdo a su estado en la firma de documentos.

4.11. Finalización de la suscripción

La suscripción finaliza con la revocación o la expiración del certificado.

5. Controles de seguridad física, instalaciones, de gestión y operacionales

5.1. Controles de seguridad física

5.1.1. Ubicación y seguridad ambiental

La infraestructura de clave pública está ubicada en el Centro de Datos de la Corte Nacional de Justicia parte de la Función Judicial, aislada físicamente del resto de servicios.

El Centro de Datos se encuentra ubicado en una instalación segura dentro del Edificio de la Corte Nacional de Justicia. Este ha sido diseñado con tecnología TIER 3, el cual permite tener un esquema redundante para precautelar la continuidad en la operación y disponibilidad de los sistemas. Cuenta con una plataforma de monitoreo (Visual Data Center) que es un centro de monitoreo centralizado de datos y herramienta de gestión de operaciones en el que se centraliza el sistema de poder, refrigeración, control ambiental, de seguridad y alarmas en una sola interfaz que permite generar las acciones preventivas y correctivas de los eventos que suceden en el Centro de Datos.

5.1.2. Gestión del acceso físico

La infraestructura de la PKI está físicamente separada de cualquier otro sistema y el acceso cuenta con un sistema de control de acceso físico de 4 niveles que dispone de los siguientes mecanismos de control:

Sistema de video seguridad que incluye video vigilancia y grabación con sistema multicámara para el monitoreo, grabación, búsqueda y reproducción con múltiples cámaras para brindar seguridad a áreas de acceso principales, periferia y monitoreo de actividades en las instalaciones.

Todas las operaciones sensibles se realizan dentro de un recinto físicamente seguro que cuenta con puertas de seguridad y control de acceso biométrico y/o contraseña de acceso.

5.1.3. Energía y aire acondicionado

5.1.3.1. Energía

Se cuenta con un grupo electrógeno capaz de soportar y suministrar la energía necesaria para el funcionamiento normal de los sistemas y equipos en caso de ausencia de suministro de energía eléctrica de la red pública.

La acometida eléctrica es independiente para los equipos del Centro de Datos y es guiada a través de tubería EMT. El local donde están instalados los equipos

de la PKI cuenta con tableros de distribución eléctrica y de alimentación de los sistemas de aire acondicionado.
Los tableros eléctricos de distribución de energía normal cuentan con un sistema de barras de cobre correctamente dimensionadas y breakers de protección y UPS. Cuenta con tableros de bypass, uno para cada equipo de protección UPS y tableros de distribución de red regulada.
Todas las acometidas eléctricas se guían a través de escalerillas metálicas fijadas al piso y con manguera BX.

5.1.3.2. Aire acondicionado

Las instalaciones donde está la infraestructura de la PKI poseen un sistema de climatización con sistemas de precisión de alto rendimiento, e incluyen equipo electrónico sensible, preciso, fiable en el control de la temperatura ambiente, la humedad y el flujo de aire para un rendimiento óptimo, con el objetivo de mantener una temperatura controlada de acuerdo con los requerimientos técnicos.

5.1.4. Exposición al agua

Las instalaciones cuentan con sistemas de piso de acceso elevado, con paneles rellenos con inyección de cemento, laminado, fórmica de alta precisión y propiedades anti fuego y antiestática.
Cuenta con controles de humedad y temperatura, sistemas de drenaje y piso elevado, para evitar el riesgo de exposición al agua.

5.1.5. Prevención y protección de incendios

El sistema de detección y extinción de incendios automático cumple con las normas UL S2203 y FM 3023436 y posee un mecanismo de control vía software con tecnología de comunicación bidireccional punto a punto con capacidad de respuesta de ¼ de segundo en la detección de incendios.
Las instalaciones cuentan con elementos de detección direccionable mediante sensores fotoeléctricos de humo y sistemas de extinción de agente limpio.

5.1.6. Seguridad de los servidores de almacenamiento

La información relacionada con los procesos de la PKI se guarda de manera segura y se dispone de servidores de respaldo con la finalidad de eliminar el riesgo asociado a una única ubicación.

Se dispone de copia fuera de los centros de procesamiento de datos de la PKI en lugares cercanos a sus instalaciones.

5.1.7. Tratamiento de residuos

La información contenida tanto en medios físicos como en soportes magnéticos que por su temporalidad y/o vigencia tecnológica debe ser eliminada, es destruida mediante procesos que precautelan la imposibilidad de su recuperación.

5.1.8. Copia de respaldos fuera de línea

Mediante un procedimiento interno de respaldo de backups fuera de línea se respalda en cintas magnéticas la información concerniente a la PKI como archivos de configuración e información de los suscriptores en registros inmutables.

5.2. Controles de procedimientos

5.2.1. Roles de confianza para la administración y operación

Para la administración y operación de la PKI existen roles estáticos fijados en cada componente con las siguientes características: no se pueden crear nuevos roles estáticos, eliminar alguno de los existentes o modificar sus acciones permitidas.

Los roles establecidos para la administración y operación de todos o parte de los componentes que integran la PKI, son los siguientes:

- **Administrador de Seguridad** que tiene la responsabilidad de administrar la implementación de políticas y prácticas de seguridad, la operación de recuperación de datos y las operaciones de archivo (*backup*) y recuperación de claves.
- **Administrador de Sistema** que está autorizado para instalar, configurar y mantener los equipos con acceso controlado a la información de seguridad y la administración de las BD del equipo.
- **Operador de Sistema** responsable de operar los sistemas y la operación de archivo (*backup*) manual de datos, pero no puede realizar la operación de *restore* de datos, ni las operaciones de *backup* manual y *restore* de claves, las cuales, debido a sus implicaciones de seguridad, sólo podrán ser realizadas por el rol Administrador de Seguridad. Además, puede realizar la monitorización y administración del hardware y software del equipo y de administración de sus servicios y crones. Si es operador en la

CA Raíz o en la CA Subordinada tiene permisos para generar manualmente las CRL y consultar las CRL emitidas.

- **Auditor** autorizado para consulta de *logs* (archivos) y para mantener los registros de auditoría de los sistemas.
- **Operador de Certificados** encargado de administrar el ciclo de vida de los certificados: generación o emisión, renovación y reemisión de certificados; así como revocación, suspensión y reactivación de los certificados.

El personal que labora en ICERT-EC es sometido a estrictos procedimientos de control, así mismo periódicamente se asignan funciones y roles para ejercer un mecanismo de oposición y de esta manera evitar el cometimiento de actos fraudulentos que atenten contra la operación de la entidad de certificación.

5.2.2. Número de personas asignado por tarea

ICERT-EC garantiza que al menos dos personas (principal y backup) se encuentran capacitados y habilitados para las operaciones relacionadas a la emisión, revocación y suspensión de certificados de firma electrónica. Por otra parte, las tareas inherentes al monitoreo y salud de la infraestructura PKI y sus aplicativos son ejecutados por especialistas en el ramo capacitados en las tares de generación, recuperación y respaldo de la clave privada de las Autoridades de Certificación raíz e intermedias.

5.2.3. Identificación y autenticación por cada rol

El auditor de ICERT-EC, precautela que las funciones y roles asignados a cada una de las personas se realicen de acuerdo con las mejores prácticas y de manera adecuada. Así mismo, se controla el acceso a la operación y administración de todos los componentes de la PKI mediante autenticación múltiple para ejecutar las tareas sensibles permitidas de acuerdo con el rol asignado.

5.2.4. Roles que requieren separación de tareas

Las siguientes tareas son ejecutadas al menos por dos personas, estas son:

- El auditor no ejecutará operaciones y/o administración de los sistemas que conforman la PKI de ICERT-EC.
- Las tareas de emisión y revocación de certificados de firma electrónica deben ser ejecutadas por dos personas distintas que ejerzan el mecanismo de oposición.

- La administración de la infraestructura y la operación de los sistemas serán tareas incompatibles que serán solventados por al menos 2 personas distintas.

5.3. Controles del personal

5.3.1. Requisitos, cualificaciones y experiencia

Los requisitos de calificación que cumple el personal que desempeña las distintas actividades en el proceso de certificación de la ICERT-EC son los siguientes:

- Título profesional o experiencia equivalente.
- Conocimiento y experiencia en certificados digitales y firma digital.
- Capacitación específica para la función desempeñada.

5.3.2. Verificación de antecedentes

El personal que desempeña las funciones operativas en el funcionamiento de la ICERTEC deberá demostrar documentadamente su formación académica, su experiencia profesional y sus conocimientos y experiencia en el desarrollo de las funciones técnicas encomendadas.

5.3.3. Capacitación y entrenamiento

Adicionalmente al conocimiento de los documentos DPC y PC de la Entidad, legislación vinculante ecuatoriana y los conocimientos de que dispone el personal se ajustan, pero no se limitan a:

- Conceptos acerca de PKI.
- Servicios prestados por la ICERT-EC.
- Aspectos legales relativos a la prestación de servicios de certificación digital.
- Seguridades física y lógica de las tareas y roles.
- Procedimientos para la operación, administración y mantenimiento de acuerdo con cada rol específico.
- Gestión de incidencias.
- Procedimientos para la operación en caso de desastres y continuidad del negocio.
- Procedimiento de gestión y de seguridad relacionada al tratamiento de los datos de carácter personal.
- Requerimientos y frecuencia de actualización formativa.
- ICERT-EC, actualiza en sus conocimientos al personal con el que cuenta cuando las condiciones lo ameritan; esto es, cuando se

realizan modificaciones importantes en las tareas de certificación, así mismo evalúa al personal de manera permanente y refuerza sus conocimientos en materia de operación y legislación ecuatoriana y mejores prácticas de certificación.

5.3.4. Rotación de roles

Para precautelar la adecuada operación de la PKI en procesos operativos se podrá realizar la rotación de funciones entre los diferentes roles asignados con intervalos y secuencias de rotación previamente definidos, no así para los roles de administración de la infraestructura PKI.

5.3.5. Sanciones en caso de acciones no autorizadas

La administración de la ICERT-EC ha estipulado la imposición de sanciones contra el personal por la ejecución de actividades no autorizadas en su respectivo rol.

5.3.6. Requerimientos para la contratación de profesionales

Todo el personal que colabora con ICERT-EC debe firmar un convenio de confidencialidad antes de comenzar sus actividades en el marco del cumplimiento de la legislación ecuatoriana y las mejores prácticas de certificación. Además, el personal recibe una formación inicial relativa al desenvolvimiento de las tareas y procesos que desarrolla la ICERT-EC; así mismo, el personal de manera permanente tendrá acceso a documentación actualizada durante su formación inicial para su conocimiento y aplicación.

5.4. Procedimientos de registro de auditoria – Controles de auditoría

Los equipos de los componentes de la PKI generarán registros de auditoría que son almacenados en las correspondientes bases de datos y en ficheros locales.

5.4.1. Tipos de eventos registrados y auditados

Los siguientes son algunos de los registros de auditoría que se almacenan con respecto a la operación de la infraestructura y software de la entidad de certificación ICERT-EC:

- Los accesos a los componentes de la PKI por los administradores y operadores.
- Las solicitudes de emisión, suspensión, reactivación y revocación de certificados y el administrador u operador que ejecutó la acción.
- La generación o renovación de certificados.
- La generación o revocación de claves.

- La actualización de la CRL y su publicación.
- Intentos de modificar o borrar la información de los titulares de certificados.
- Back up, archivo y restauración.
- Cambios en la configuración del sistema - Actualizaciones de software y hardware.
- Mantenimiento del sistema. - Cambios de personal - Gestión de usuarios.
- Control de acceso a la infraestructura de la PKI

Los registros incluyen los siguientes elementos:

- Fecha y hora de la entrada.
- Identidad digital que ingresa en los sistemas.
- Secuencia de la entrada y eventos ejecutados.
- Tipo de entrada.

5.4.2. Frecuencia de procesamiento de los registros de auditoría

La frecuencia para realizar el análisis y procesamiento de los registros de auditoría será determinada por la Subdirección Nacional de Seguridad de la Información del Consejo de la Judicatura.

Adicionalmente, se revisan los logs de auditoría para la resolución de incidentes cuando se produce una alerta en la operación de la infraestructura y/o el software de la PKI. Los registros de auditoría se encuentran centralizados y permite un análisis profundo a través de su inspección; así mismo, estos eventos se registran en una bitácora de incidentes que son reportados de manera mensual.

Por otra parte, se cuenta con un *Plan de Respaldos* que contempla la remoción de los registros de auditoría periódicamente los cuales son almacenados remotamente antes de ser almacenados en cintas; todo esto, con el objetivo de establecer un espacio de almacenamiento de logs en los equipos de la PKI de al menos los últimos 3 meses de operación.

5.4.3. Período de resguardo de los registros de auditoría

Los registros de auditoría se conservarán durante todo el ciclo de vida de la PKI y la ICERT-EC. Dependiendo de la sensibilidad de la información se ha establecido períodos de destrucción de la información de manera segura que oscila entre 1 año y 10 años.

5.4.4. Protección de los registros de auditoría

La información de los registros de eventos se encuentra protegida por mecanismos de firma y cifrado.

Únicamente el Auditor tiene acceso a los registros auditados. Ningún operador tiene permisos para modificar o borrar los registros.

5.4.5. Procedimiento de copia de respaldo de los registros de auditoría

La ICERT-EC genera copias diarias locales y en sitio remoto de los registros de auditoría. Los archivos de respaldo de las auditorías se guardan en el centro de datos de la PKI.

5.4.6. Sistemas de recolección de información de auditoría

La recolección de información de auditoría es una combinación de procesos automáticos, ejecutados por los sistemas y aplicaciones de la ICERT-EC, y procesos manuales ejecutados por los operadores autorizados para tales funciones.

5.4.7. Sistemas de revisión de eventos

La ICERT-EC dispone de las herramientas apropiadas para la revisión de los eventos auditados para facilitar la detección de eventos rutinarios o excepcionales.

5.4.8. Análisis de vulnerabilidades

La PKI se encuentra resguardada por una arquitectura de seguridad informática que protege la infraestructura de tecnología del Consejo de la Judicatura; de esta forma cuenta con sistemas y herramientas que identifican potenciales ataques que podrían vulnerar los sistemas. La presentación del resultado del análisis de vulnerabilidades implica corregir las vulnerabilidades detectadas y la emisión de los correspondientes informes a la autoridad de la ICERT-EC.

Se establece en seis (6) meses el periodo máximo de la realización de análisis de vulnerabilidades y de seguridad perimetral.

5.5. Almacenamiento y archivo de la información

5.5.1. Tipo de información a resguardar

Dando cumplimiento a la regulación vigente sobre la materia, en la ICERT-EC se guardan archivos relacionados con el ciclo de vida de los certificados, entre los que se encuentran:

- Las solicitudes de certificados.

- El contrato suscrito.
- Los datos suministrados y la información de soporte entregada.
- CRLs emitidas o registros del estado de los certificados generados.
- Datos de auditoría del sistema.

5.5.2. Período de resguardo de la información

En la ICERT-EC los datos acerca del ciclo de vida de los certificados emitidos son archivados por un período mínimo de cinco (5) años, para información referente a documentación de solicitudes archivadas por un periodo máximo de un (1) año.

5.5.3. Protección de la información archivada

Para el acceso a la información archivada se cuenta con controles tecnológicos y procedimentales mediante el cual se protege la información con niveles de acceso que previenen la modificación, borrado o alteración de la documentación archivada.

5.5.4. Procedimiento de respaldo de la información

Se cuenta con un *Plan de Respaldos* mediante el cual se estipula que se realizan copias diarias de los ficheros de los archivos a resguardar de la ICERT-EC. Se guarda una copia en el Centro de Datos en Quito y una segunda copia cifrada se guarda en el Centro de Datos en Cuenca.

5.5.5. Sello de tiempo para los archivos

Los registros fechados mediante sello de tiempo cuentan con una fuente confiable mediante el protocolo NTP en comunicación con el INOCAR.

5.5.6. Sistemas de almacenamiento

Toda la información relacionada con la auditoría en la ICERT-EC es interna y se encuentra centralizada y archivada en sus propias instalaciones. Así mismo, se considera almacenamiento en nube siempre y cuando esta garantice adecuados niveles de seguridad y sostenibilidad en el tiempo.

5.5.7. Procedimiento para obtener y verificar la información archivada

Se dispone de un procedimiento interno para la verificación de la información almacenada con el objetivo de validar que la información archivada es correcta y accesible. Así mismo, se crea una incidencia en el caso de error o comportamientos imprevistos.

5.6. Cambio de clave

Únicamente si se produce un cambio de la clave pública de la ICERT-EC se procederá a notificar a los usuarios de la CA. Este procedimiento es el mismo que el utilizado para proporcionar la clave inicial.

5.7. Compromiso de claves y recuperación ante desastres

5.7.1. Procedimientos para administrar incidentes

La Entidad de Certificación ICERT-EC dispone de un *Plan de Continuidad del Negocio* que garantiza mantener o restaurar sus operaciones luego de una interrupción, falla o proceso crítico.

En caso de que se produjese un incidente que implique la indisponibilidad de los servicios de certificación se procederá a la ejecución del *Plan de continuidad del negocio*, el mismo que garantiza que los servicios considerados como críticos por su requerimiento de disponibilidad estén habilitados en el plazo de setenta y dos (72) horas.

5.7.2. Recursos informáticos, software y datos corruptos

Si los componentes de la PKI (hardware), el software y/o los datos son alterados o se sospecha que son corruptos se suspenderá el funcionamiento de los servicios de la ICERT-EC hasta que sea restablecido el entorno seguro, determinando cuáles certificados serán revocados. Si la clave de la CA debe ser revocada, la nueva clave pública será suministrada nuevamente a los usuarios y los suscriptores serán nuevamente registrados.

5.7.3. Procedimientos ante compromiso de la clave privada de la CA

En el supuesto de revocación del certificado de la CA si la clave privada ha sido comprometida se generará y publicará la correspondiente CRL, se suspenderá el funcionamiento de la Entidad y se procederá a generar una nueva entidad con un nuevo par de claves. El certificado revocado permanecerá accesible en el repositorio de la ICERT-EC con el objeto de permitir la verificación de los certificados emitidos durante su período de funcionamiento.

Del particular se informará a las entidades correspondientes.

5.7.4. Capacidad de continuidad del negocio ante un desastre

La ICERT-EC garantiza su capacidad para asegurar la continuidad de sus operaciones si se produjera un desastre natural, como un terremoto que destruya las instalaciones, o desastre de cualquier tipo que comprometa su funcionamiento. Existe una infraestructura redundante para precautelar las operaciones.

5.7.5. Medidas para la corrección de vulnerabilidades detectadas

Los servicios de las interfaces web de administración y operación de todos los componentes de la infraestructura PKI y de la interfaz web de usuarios de la RA aplican filtros para impedir que puedan contener código intruso para vulnerar la base de datos. Las actualizaciones de software en los componentes de la infraestructura PKI vienen firmados para evitar que se introduzca código malicioso dentro de los entornos de producción de la Entidad de Certificación ICERT-EC.

Los servicios de las interfaces web de administración y operación de todos los componentes de la PKI y de la interfaz web de usuarios de la RA aplican filtros a todas las páginas que puedan recibir parámetros a través del método GET, incluidos en la URL, para impedir que puedan contener código intruso, que pudiese producir, por ejemplo, un ataque de inyección SQL.

5.8. Terminación o disolución de las autoridades de certificación y de registro

Las causas que pueden producir el cese de la actividad de la ICERT-EC son:

- Compromiso de la clave privada de la CA.
- Decisión propia de la ICERT-EC.

En el supuesto no consentido y muy remoto de la disolución de la Entidad de Certificación ICERT-EC, el procedimiento a seguir será determinado por la Subdirección Nacional de Seguridad de la Información de la Dirección Nacional de Tecnologías de la Información y Comunicaciones del Consejo de la Judicatura y el titular de la Dirección Nacional de Tecnologías en conjunto con el respectivo informe debidamente motivado y de acción indelegable a otro funcionario de acuerdo a las competencias estatutarias, poniendo en conocimiento además de la máxima autoridad institucional sobre esta decisión.

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, permitiendo 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 contrato legalizado:

- 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.
- Entrega de clave pública en base a petición de certificados en formato PKCS #10. Claves generadas por el suscriptor bajo sus propios medios.
- 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 genera en dispositivos criptográficos hardware con certificación FIPS 140-2 Nivel 3 y/o Common Criteria EAL4+ (CWA14169).

6.1.2. Claves de la CA

El par de claves de la CA Raíz y la CA Subordinada se genera de acuerdo con el procedimiento de ceremonia de generación de claves desarrollada por la institución.

El proceso de generación de claves es realizado por personal autorizado de la Entidad de Certificación ICERT-EC según los roles de confianza utilizando un HSM (Módulo de Hardware Criptográfico, con certificación de seguridad FIPS 140-2 nivel 3 y/o Common Criteria EAL4+) el cual utiliza el estándar AIS20 para la generación de números aleatorios.

La CA Raíz permanece apagada y solo es utilizada para la emisión de ARL con un periodo de validez de seis (6) meses o cada que se genere un certificado de CA subordinada, en todo momento este elemento no tiene conexión a red.

6.1.3. Claves del suscriptor

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

- Generación y entrega del par de claves y certificado en dispositivo token / tarjeta criptográfica. Este dispositivo permite el uso de las claves privadas y posee una clave de autenticación (PIN) de conocimiento y uso exclusivo del suscriptor para garantizar que los datos de creación de firma estén protegidos frente a terceros.
- Generación del par de claves por parte de la ICERT-EC y entrega del par de claves y certificado en archivo con formato PKCS #12.
- Generación del par de claves y certificado en un HSM PKCS#11 (SFC) y almacenamiento seguro de las claves. Estas claves cifradas serán solamente utilizables a través de un software seguro destinado a este propósito y previa autenticación mediante credenciales del suscriptor.
- Generación de la llave pública en base a una petición CSR PKCS #10, donde las claves son generadas por el suscriptor mediante sus propios medios.

6.1.4. 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 la 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 conoce.

En el caso de certificados bajo petición CSR PKCS#10, las claves son generadas por el suscriptor bajo sus propios medios y el certificado es emitido por la CA.

6.1.5. Tamaño de las claves

El algoritmo utilizado para la generación de claves es el RSA y el tamaño de claves se detalla a continuación:

Usuario	Tipo de certificado	Tamaño de clave

Autoridades de Certificación	CA Raíz, AC Subordinada, ARL (CA Raíz), CRL (CA Subordinada)	4096 bits
Personas	Persona Natural, Persona Jurídica Privada, Persona Jurídica Pública, Miembro de Empresa	2048 bits
Entidades	Empresa o Institución	2048 bits
Unidades Organizativas	Departamento de Empresa o Institución	2048 bits
Dispositivos	TSA, VA, Servidor Web Genérico	2048 bits

6.2. Protección de clave privada

La clave privada de la CA es almacenada en el módulo criptográfico HSM y se mantiene cifrada y el acceso a la clave con la que se realizó el cifrado está restringido a personal autorizado según los roles de administración de la infraestructura PKI de la ICERT-EC.

6.2.1. Controles y estándares para los módulos criptográficos

Los módulos utilizados para la creación de las claves a utilizar por las autoridades de certificación disponen de un nivel de seguridad que garantiza su funcionalidad y seguridad.

El módulo criptográfico HSM que posee certificaciones de seguridad estándar FIPS 140-2 del NIST, Nivel 3 y/o Common Criteria EAL4+ es el utilizado para control de protección de las claves privadas de la CA.

6.2.2. Control multipersona sobre la clave privada

El acceso a la clave privada utilizada por la CA Raíz y la CA subordinada se realiza con la participación de por lo menos 2 personas para tareas sensibles, lo que garantiza que ninguna persona en particular tiene el control o la facultad individual para activar o utilizar dichas claves privadas. Adicional a ello existe un custodio de respaldos de la clave privada que es guardada en dos cajas fuertes, en sitio principal y alterno, que no es ninguna de las personas mencionadas anteriormente.

6.2.3. Controles sobre la clave privada de la CA

Actividad	Descripción
Copia de seguridad de la clave privada	Las copias de respaldo de las claves privadas se almacenan cifradas en dos sitios alternos a los centros de datos de Quito y Cuenca cercanos a cada uno de ellos. Existe por lo menos una copia de respaldo de las claves privadas de la CA que permite su recuperación en caso de desastre, que es almacenada y recuperada por el personal autorizado según los roles de confianza y con la presencia de un custodio de claves.
Archivo de la clave privada	Las claves privadas de las Autoridades de Certificación y Autoridad de Registro se guardan en dispositivos de hardware criptográfico con certificación de seguridad FIPS 140-2 nivel 3 y/o Common Criteria EAL4+) y sus copias en cajas fuertes.
Introducción de la clave privada al módulo criptográfico	La clave privada se crea dentro del módulo criptográfico en el momento de la creación de cada una de las entidades de la ICERT-EC que hace uso de dichos módulos.
Activación de la clave privada	Las claves privadas de las autoridades de certificación se activan mediante la inicialización del software de CA y la activación del hardware criptográfico que contiene las claves.
Desactivación de la clave privada	La desactivación de la clave privada de las Autoridades de Certificación se puede producir por la detención del software de la CA.
Destrucción de clave privada	La destrucción de la clave privada puede realizarse por el borrado de las claves de los HSM que las contiene.

6.2.4. Controles sobre la clave privada de los suscriptores

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	PKCS#10 (HSM Genérico)
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/descrifrada por una clave sólo conocida y custodiada en el HSM. Sólo el suscriptor dispone de los mecanismos para su uso.	ICERT-EC no realiza respaldo sobre las claves privadas de los suscriptores generadas por el suscriptor mediante sus propios medios.
Almacenamiento	Las claves privadas de los suscriptores generadas en dispositivo token o tarjeta criptográfica	Las claves privadas de los suscriptores contenidas en archivos PKCS #12 NUNCA son	Las claves privadas de los suscriptores generadas en HSM son almacenadas en una base de datos	Las claves privadas generadas mediante una petición PKCS#10 NUNCA son

de la clave privada	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.	almacenadas por ICERT-EC. El archivo PKCS #12 se envía al suscriptor para que éste lo almacene y conserve.	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.	almacenadas por ICERT-EC.

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.	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	La clave privada permanece siempre en posesión del suscriptor, por lo que la ICERT-EC nunca tiene acceso a la misma.

		El archivo PKCS #12 protege el uso de la clave privada a través de una clave que es custodiada por el suscriptor.	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.	La activación del uso de la clave privada generada por el suscriptor en sus propios medios es realizada por él mismo.
Desactivación de la clave privada	El método para desactivar la clave privada del suscriptor es retirar el dispositivo token/tarjeta	El método para desactivar la clave privada del suscriptor que ha importado su certificado a	El método para desactivar la clave privada del suscriptor es mediante el	El método para desactivar la clave privada del suscriptor es mediante

	criptográfica del equipo, inmediatamente cualquier contenido asociado queda deshabilitado incluyendo la clave privada.	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.	cierre de sesión abierta con el SFC.	el procedimiento establecido por el propio suscriptor.
Destrucción de la 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.	La destrucción de la clave privada es mediante la eliminación de la clave privada.

6.3. Otros aspectos de la gestión del par de claves

6.3.1. Archivo de la clave pública

La Entidad de Certificación ICERT-EC mantiene el archivo de todos los certificados emitidos por el período de vigencia de los certificados.

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

El certificado de la CA Raíz tiene una validez de 20 años y el de la CA Subordinada de *notAfter* del Certificado de CA Raíz y hora local 00:00:00

codificado en UTCTime. El certificado de la RA tiene una validez *notAfter* del certificado de CA Subordinada CJ – 1 hora, codificado en UTCTime. El periodo de validez de los certificados de suscriptores queda establecido en las respectivas políticas de certificados.

El par de claves tiene vigencia mientras exista un certificado válido que las sustente.

6.4. Datos de activación

Los datos de activación de las CA de la ICERT-EC se generan y almacenan en *smartcard* criptográficas entregadas a personal autorizado. Solo el personal autorizado conoce los PIN y contraseñas para acceder a los datos de activación.

La protección de los datos de activación previene el uso no autorizado de la clave privada.

6.5. Controles de seguridad informática

Los controles de seguridad informática establecidos en la ICERT-EC se consideran información sensible y confidencial. ICERT-EC dispone de un sistema de gestión de seguridad de la información basado en la ISO-27001, del cual se resalta los siguientes aspectos:

- Control de acceso a los servicios de la CA.
- Identificación y autenticación de usuarios para las aplicaciones de la CA a partir de certificados digitales.
- Auditoría de eventos relativos a la seguridad.
- Mecanismos de recuperación de claves y del sistema de la CA.
- Configuración de seguridad de las aplicaciones.
- Configuración de usuarios y privilegios.
- Gestión de privilegios para asignar las tareas según el rol.
- Plan de mantenimiento de la infraestructura PKI.
- Plan de contingencia y recuperación de desastres.

6.6 Controles técnicos de seguridad del ciclo de vida

6.6.1 Controles de desarrollo de sistemas

Los controles de desarrollo del sistema incluyen la seguridad de la gestión de configuración y las prácticas de ingeniería de software en los entornos de producción, test y contingencia. Así mismo, en el marco del Sistema de Gestión de Seguridad de la Información de ICERT-EC se siguen metodologías de desarrollo seguro.

6.6.2 Controles de gestión de seguridad

Entre los controles implementados para gestionar el ciclo de vida de los certificados se resaltan al menos los siguientes:

- Concientización en materia de seguridad de la información a los colaboradores de ICERT-EC.
- Clasificación de los activos de información de ICERT-EC, según su nivel de sensibilidad.
- Gestión del control de acceso a los activos de información identificados mediante medidas técnicas y procedimentales.
- Medidas de seguridad exigidos a los proveedores de infraestructura, software y servicios relacionados que prestan su contingente a ICERT-EC.
- Control y monitoreo permanente de las capacidades de la PKI.
- Atención de incidentes y de las vulnerabilidades técnicas.
- Medidas de control técnico como antivirus y firewall para evitar ataques externos.
- Multifactor de autenticación para el acceso a los componentes sensibles de la PKI.
- Segregación de funciones de los colaboradores de ICERT-EC de tal forma que se genere un mecanismo de oposición en las actividades como emisión y revocación de los certificados de firma electrónica.
- Controles de seguridad perimetral tanto física como lógica a la PKI.

Las afectaciones a la infraestructura como actualización y configuración de los sistemas que conforman la PKI son autorizadas por la máxima autoridad de ICERT-EC que es el Subdirector de Seguridad de la Información y se encuentran documentadas y controladas.

6.7. Controles de seguridad de la red

El control de acceso a la red está permitido únicamente a personal autorizado.

Los componentes de la red se encuentran ubicados en instalaciones seguras con monitoreo y vigilancia permanente en donde se garantiza su integridad.

La red está protegida mediante firewall de red que cuenta con sistemas IPS, Antibot, Application control, URL filtering, antivirus además de un balanceador de carga para mejorar el rendimiento y disponibilidad de los servicios web para mejorar el rendimiento y disponibilidad de los servicios web; infraestructura que en conjunto impiden ataques como DoS, DDoS, ataques MitM e inyecciones SQL.

6.8. Controles de ingeniería de los módulos criptográficos

Los módulos criptográficos utilizados por la ICERT-EC cumplen los parámetros de certificación exigidos para garantizar la seguridad de las actividades desarrolladas.

Las operaciones de criptografía de ICERT-EC son realizadas en módulos con las certificaciones FIPS 140-2 nivel 3.

6.9. Sello de tiempo

La firma de datos puede incluir un sello de tiempo generado por la TSA, que consiste en la 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.

7. Perfiles de certificados, listas de revocación y OCSP

7.1. Perfiles de certificado

7.1.1. Número de versión

El formato de los distintos tipos de certificados emitidos por la CA Raíz y la CA Subordinada de la ICERT-EC, incluyendo los certificados auto firmados de la CA Raíz, será X.509 v3, conforme al estándar RFC 5280.

7.1.2. Extensiones del certificado

Podrán incluir únicamente las extensiones de certificado definidas en [RFC5280] que están indicadas en los perfiles de certificado especificados en [P-CERT], a saber:

- authorityKeyIdentifier
- subjectKeyIdentifier
- keyUsage

- certificatePolicies
- subjectAltName
- basicConstraints
- extKeyUsage
- cRLDistributionPoints
- authorityInformationAccess

CERTIFICADO DE AC RAÍZ CJ

CERTIFICADO DE CA RAÍZ CJ	
Componente	**Valor**
Extensiones de certificado X.509 v3 (extensions)	
subjectKeyIdentifier	73 c8 c3 bd 0f f9 55 40 f1 65 98 7a 58 a3 67 48 1f 70 9d 1b
keyUsage (critical)	keyCertSign cRLSign
certificatePolicies	
policyIdentifier	2.5.29.32.0 (anyPolicy)
policyQualifiers	
policyQualifierId	id-qt-cps
qualifier-cPSuri	http://www.icert.fje.gob.ec/dpc/declaracion_practicas_certificacion.pdf
basicConstraints (critical)	
CA	TRUE

keyIdentifier	2f 22 7a f8 5e 6d 94 8e 6a 40 14 37 c7 6e 6b 72 e9 3a c2 3f
subjectKeyIdentifier	29 b4 60 33 fb 0d c6 c2 5a 42 7b 1d a1 35 bc 80 2e db 65 c8
keyUsage (critical)	keyCertSign cRLSign
certificatePolicies	
policyIdentifier	2.5.29.32.0 (anyPolicy)
policyQualifiers	
policyQualifierId	id-qt-cps
qualifier-cPSuri	http://www.icert.fje.gob.ec/dpc/declaracion_practicas_certificacion.pdf
basicConstraints(critical)	
CA	TRUE
pathLenConstraint	0
CRLDistributionPoints	
distributionPoint-fullName	
uniformResourceIdentifier	http://www.icert.fje.gob.ec/crl/arl_icert.crl

CERTIFICADO DE CA SUBORDINADA CJ

CERTIFICADO DE CA SUBORDINADA CJ	
Componente	**Valor**
Extensiones de certificado X.509 v3 (extensions)	
authorityKeyIdentifier	

CERTIFICADO DE TSA CJ

CERTIFICADO DE TSA CJ	
Componente	**Valor**
Extensiones de certificado X.509 v3 (extensions)	
authorityKeyIdentifier	
keyIdentifier	2f 22 7a f8 5e 6d 94 8e 6a 40 14 37 c7 6e 6b 72 e9 3a c2 3f
subjectKeyIdentifier	29 b4 60 33 fb 0d c6 c2 5a 42 7b 1d a1 35 bc 80 2e db 65 c8
keyUsage (critical)	digitalSignature nonRepudiation

certificatePolicies	
policyIdentifier	1.3.6.1.4.1.43745.1.2.4.1.1.3
policyQualifiers	
policyQualifierId	id-qt-cps
qualifier-cPSuri	http://www.icert.fje.gob.ec/dpc/declaracion_practicas_certificacion.pdf
basicConstraints	
extKeyUsage (critical)	id-kp-timeStamping
CRLDistributionPoints	
distributionPoint-fullName	
uniformResourceIdentifier	http://www.icert.fje.gob.ec/crl/icert.crl
authorityInfoAccess	
accessMethod	id-ad-ocsp
accessLocation uniformResourceIdentifier	~~http://ocsp.icert.fje.g~~ob.ec

CERTIFICADO DE VA CJ

CERTIFICADO DE VA CJ	
Componente	**Valor**
Extensiones de certificado X.509 v3 (extensions)	

authorityKeyIdentifier	
keyIdentifier	2f 22 7a f8 5e 6d 94 8e 6a 40 14 37 c7 6e 6b 72 e9 3a c2 3f
subjectKeyIdentifier	29 b4 60 33 fb 0d c6 c2 5a 42 7b 1d a1 35 bc 80 2e db 65 c8
keyUsage (critical)	digitalSignature nonRepudiation
certificatePolicies	
policyIdentifier	1.3.6.1.4.1.43745.1.2.4.2.1.3
policyQualifiers	
policyQualifierId	id-qt-cps

qualifier-cPSuri	http://www.icert.fje.gob.ec/dpc/declaracion_practicas_certificacion.pdf
basicConstraints	
extKeyUsage (critical)	id-kp-OCSPSigning
cRLDistributionPoints	
distributionPoint-fullName	
uniformResourceIdentifier	http://www.icert.fje.gob.ec/crl/icert.crl

En cada una de las políticas de certificados, para los certificados de usuario final se describe los campos y extensiones utilizadas por los diferentes tipos de certificado.

7.1.3. Identificadores de objeto del algoritmo

OID del algoritmo de firma sha256 with RSA Encryption

OID del algoritmo de la clave pública RSA Encryption

7.1.4. Formatos de nombres

El formato de nombres en los certificados digitales emitidos por la ICERT-EC contiene el *distinguished name* del emisor y del suscriptor del certificado en los campos *issuer name* y *subject name*, respectivamente.

7.1.5. Restricciones de nombre

De acuerdo a la recomendación X.500 para nombres en certificados digitales estos deben ser únicos y no ambiguos.

7.1.6. Objeto identificador de la Declaración de Prácticas de Certificación

La ICERT-EC tiene asignado el OID 43745 desde mayo de 2014 registrado ante la IANA (*Internet Assigned Numbers Authority*).

El OID correspondiente a este documento, Declaración de Prácticas de Certificación, es el siguiente: 1.3.6.1.4.1 43745.1.2.1.1

Además, cada política de certificados tiene asignado su correspondiente OID a partir de la raíz 43745.

7.1.7. Sintaxis y semántica de los calificadores de la política

No estipulado.

7.2. Perfil de las Listas de Certificados Revocados CRL

El formato de las CRL emitidas por la CA Raíz (ARL) y la CA Subordinada será X.509 v2, conforme al estándar [RFC5280], con las siguientes restricciones en sus componentes:

- Campos de CRL (elementos del componente tbsCertList de las CRL, excluyendo el elemento crlExtensions).
- Extensiones de CRL (componentes del elemento crlExtensions, en el componente tbsCertList de las CRL).

7.2.1. Número de versión

Las CRL se emiten de acuerdo al estándar X.509 v2.

7.2.2. Extensiones de las CRL

ARL (CA RAÍZ)

Extensiones de CRL X.509 v2 (crlExtensions)	
authorityKeyIdentifier	
keyIdentifier	73 c8 c3 bd 0f f9 55 40 f1 65 98 7a 58 a3 67 48 1f 70 9d 1b
CRLNumber	Número entero secuencial (valor inicial: 00)

CRL (CA Subordinada)

Extensiones de CRL X.509 v2 (crlExtensions)	
authorityKeyIdentifier	
keyIdentifier	2f 22 7a f8 5e 6d 94 8e 6a 40 14 37 c7 6e 6b 72 e9 3a c2 3f
cRLNumber	Número entero secuencial (valor inicial: 00)

7.3. Perfil de OCSP

La utilización del protocolo OCSP según lo estipulado en la RFC 2560 está descrito en el documento interno Administración de OCSP.

7.3.1. Número de versión

El certificado OCSP se emite de acuerdo al estándar X509 v3.

7.3.2. Extensiones de OCSP

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

keyUsage	crítica
basicConstraints	crítica

8. Auditorías de conformidad y otras valoraciones

8.1. Frecuencia y circunstancias de las auditorías

La ICERT-EC realiza auditorías internas para precautelar el adecuado funcionamiento de la infraestructura tecnológica y operativa de la Entidad de Certificación para dar cumplimiento con lo estipulado en la presente Declaración de Prácticas de Certificación y las correspondientes políticas de certificado, así como en la Declaración de Políticas de Seguridad.

El auditor interno no debe tener relación funcional con el área objeto de la auditoría.

8.2. Identidad y calificaciones de los auditores

Se realizará además una auditoría externa para verificar el cumplimiento de los requisitos de seguridad y operativos para autoridades certificadoras.

Las auditorías externas son realizadas por empresas existentes en el mercado y especialistas en la materia.

8.3. Relación entre el auditor y la entidad evaluada

La empresa auditora y la Entidad de Certificación no deberán tener ninguna relación que pueda originar un conflicto de intereses.

8.4. Temas cubiertos en la valoración

La auditoría debe determinar si los servicios brindados por la ICERT-EC se adecúan a lo establecido en la DPC y las PC aplicables a cada tipo de certificado y se realiza sobre los siguientes aspectos:

- Publicación de la información relativa a la Declaración de Prácticas de Certificación y las políticas de certificados y las correspondientes modificaciones y actualizaciones.

- Control sobre la integridad de las claves pública y privada, así como de la gestión de los certificados.
- Cumplimiento de los controles de seguridad establecidos en esta Declaración de Prácticas de Certificación estipulados en el acápite número 5. Otros aspectos cubiertos por una auditoría son:
  - o Políticas de seguridad.
  - o Seguridad física.
  - o Evaluación tecnológica.
  - o Administración de los servicios brindados por la CA.
  - o DPC y PC vigentes
  - o Política de privacidad.

8.5. No conformidades

Del resultado de las auditorías acerca de no conformidades se tomará acciones inmediatas para subsanarlas en el menor tiempo posible.

8.6. Comunicación de resultados

Es responsabilidad del auditor informar acerca de los resultados de la auditoría a la instancia responsable del área donde se detecte la no conformidad, a la respectiva autoridad.

9. Otros asuntos comerciales y legales

9.1. Tarifas

9.1.1. Tarifas de emisión o renovación de certificados

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.

9.1.2. Tarifas de acceso a los certificados

No existe una tarifa para el acceso a los certificados emitidos por la ICERT-EC.

9.1.3. Tarifas de acceso a la información de estado o revocación

No existe una tarifa para el acceso a la información publicada acerca del estado de los certificados emitidos por la ICERT-EC en la CRL.

9.1.4. Tarifas por otros servicios

Las tarifas por otros servicios se encuentran publicadas en la página web de la ICERT-EC en la siguiente ubicación: http://www.icert.fje.gob.ec sección tarifas.

9.1.5. Política de rembolso

A determinar por la Subdirección Nacional de Seguridad de la Información del Consejo de la Judicatura y su responsable.

9.2. Responsabilidad financiera

ICERT-EC mantiene una póliza de responsabilidad civil para responder ante cualquier eventualidad que signifique un perjuicio para los suscriptores, siempre y cuando los daños y perjuicios se deriven de errores, omisiones o actos negligentes por parte de la misma.

Se aclara que ICERT-EC no se responsabiliza por actos relacionados con el incumplimiento o ejecución incorrecta de las obligaciones contraídas por el suscriptor y/o usuario de un certificado de firma, y por la incorrecta utilización de sus certificados digitales, así como de sus claves privadas.

9.3. Información confidencial de los negocios

La ICERT-EC garantiza que la información cursada entre los usuarios de los certificados de firma y terceros que confían, tales como planes de negocios, información de ventas, secretos comerciales y otros, es confidencial y de uso exclusivo por parte de los interesados.

Los operadores de las entidades CA y RA están comprometidos a no revelar toda la información relativa al certificado de firma a terceros.

9.3.1. Alcance de la información confidencial

La ICERT-EC considera como información confidencial que no podrá ser divulgada a terceros a:

- Las claves privadas de las entidades que forman la ICERT-EC.
- Las claves privadas de los suscriptores que la ICERT-EC mantiene en custodia.
- La información personal de suscriptores que no está contenida en el certificado digital.
- La información relativa a las operaciones que lleva a cabo la ICERT-EC.
- La información acerca de los parámetros de seguridad, controles y procedimientos de auditoría.
- El Manual de Seguridad y Procedimientos Internos de la ICERT-EC.
- Plan de contingencias y continuidad de negocio.

9.3.2. Información no confidencial

La información que no se considera confidencial hace referencia a:

- La incluida en la Declaración de Prácticas de Certificación de la ICERT-EC.
- La incluida en las Políticas de Certificados emitidos por ICERT-EC.
- Los certificados emitidos y la información contenida en los certificados. - Las listas de certificados revocados (CRL).

9.3.3. Responsabilidad para proteger la información confidencial

El personal de la ICERT-EC que participa en las actividades relativas al funcionamiento de la infraestructura para la emisión de certificados está sujeto al deber de secreto y confidencialidad, de acuerdo a las políticas de ICERT-EC establecidas respecto de su contratación y desempeño.

9.4. Privacidad de la información personal

La información personal entregada en el proceso de solicitud y emisión de un certificado de firma es confidencial y sujeta a protección por parte de la ICERT-EC conforme a la legislación nacional relativa a la protección de datos personales.

Los datos de los usuarios serán usados única y exclusivamente para los fines indicados en el presente documento. Así mismo, se dará cumplimiento al acceso, modificación y eliminación de datos personales de los registros de ICERT-EC, bajo los procedimientos contemplados en la presente DPC.

9.4.1. Plan de privacidad

El plan de privacidad desarrollado para proteger la información considerada confidencial incluye controles para proteger y precautelar su integridad, así también, para asignarle el nivel de criticidad correspondiente.

9.4.2. Información considerada privada

ICERT-EC cataloga como información confidencial o privada aquella que no cuenta con los respectivos permisos para hacerse pública por parte de los suscriptores y partes interesadas.

9.4.3. Información no considerada privada

Se considera información no confidencial a la siguiente:

- Los certificados emitidos.
- El número de serie de los certificados emitidos.
- Los nombres y apellidos del suscriptor del certificado y cualquier otra información relativa a los fines de uso de los certificados digitales.
- El período de validez del certificado, especificando su fecha de emisión y su fecha de caducidad.

- La información relativa a su estatus y las fechas de inicio, de revocación o suspensión.
- Las listas de revocación de certificados de la ICERT-EC. - Los documentos que contienen la DPC y las PC.
- La información que la normativa vigente considera pertinente de ser publicada.

9.4.4. Responsabilidad para proteger la información privada

La información referente a usuarios y suscriptores es administrada por personal autorizado y está protegida por estrictas políticas de uso, que no sea el necesario para el desenvolvimiento de los fines para los que fue creada.

ICERT-EC precautela la protección de los datos personales obtenidos en función de sus actividades, de conformidad con lo establecido en el artículo 9 de la Ley de Comercio Electrónico, Firmas Electrónicas y Mansajes de Datos.

9.4.5. Notificación y consentimiento para el uso de información privada

Se requiere del consentimiento expreso del dueño de la información para el uso de la información privada o confidencial.

9.4.6. Divulgación de información dentro de un proceso judicial o administrativo

Únicamente por requerimiento de autoridad competente dentro de un proceso judicial o administrativo, ICERT-EC hará entrega a terceros de la información catalogada como confidencial por parte de los suscriptores.

9.5. Derechos de propiedad intelectual

Los derechos de propiedad intelectual, tales como derechos de autor, patentes, marcas registradas o secretos comerciales que los suscriptores declaran como tales o que están incluidos en los certificados, nombres, claves, DPC o PC, son protegidos por la ICERT-EC.

El suscriptor conserva la propiedad intelectual sobre las claves privadas y públicas relativas a su certificado.

Los derechos de propiedad intelectual referidos a la presente DPC, las políticas de certificado, los certificados emitidos y las CRL pertenecen a la Entidad de Certificación ICERT-EC.

9.6. Obligaciones y garantías

9.6.1. Obligaciones y garantías de la CA

ICERT-EC está obligada a:

- Contar con la infraestructura tecnológica requerida para el ejercicio de las actividades de certificación.
- Utilizar sistemas fiables que garanticen la seguridad técnica y criptográfica de los procesos de certificación.
- Utilizar sistemas fiables para el almacenamiento de certificados que permitan comprobar su autenticidad e impidan que personas no autorizadas alteren los datos y permitan detectar cualquier cambio que afecte a las condiciones de seguridad.
- Contar con los recursos económicos y humanos e instalaciones requeridas para ofrecer los servicios de certificación.
- Disponer de los controles de seguridad física, de procedimientos y estrategias necesarias para precautelar la confianza y operación de los servicios.
- Realizar sus operaciones de conformidad con esta DPC.
- Garantizar el cumplimiento de los requisitos impuestos por la legislación vigente.
- Proteger las claves privadas de la ICERT-EC.
- No copiar ni almacenar las claves privadas correspondientes a los certificados emitidos y tampoco de certificados de uso interno emitidos con el propósito de utilizarlos para firma electrónica, cuando estos sean generados sobre los dispositivos criptográficos del suscriptor.
- Emitir certificados según el estándar X.509 v3, según lo establecido en las políticas de certificado que les serán aplicables y de acuerdo a lo solicitado por el suscriptor.
- Emitir certificados que sean conformes con la información proporcionada por el solicitante previo a su emisión y libres de errores de entrada de datos.
- Precautelar la confidencialidad en el proceso de generación de datos de emisión del certificado de firma y su entrega al suscriptor por un procedimiento seguro.
- Precautelar la protección, confidencialidad y debido uso de la información suministrada por el suscriptor.
- Precautelar que se puede determinar la fecha y hora en la que se expidió o se revocó un certificado.
- Utilizar sistemas fiables para almacenar los certificados e impedir que personas no autorizadas modifiquen los datos.
- Detectar cualquier indicio que afecte la seguridad de los datos relacionados con los certificados.
- Publicar y mantener actualizado el directorio de certificados en el directorio LDAP indicando los certificados emitidos y si están vigentes o revocados.

- Almacenar en la infraestructura PKI de forma indefinida las CRL y los certificados digitales vigentes, vencidos y revocados.
- Publicar de manera oportuna en la página web los certificados que se encuentran vigentes y las CRL.
- Informar a los suscriptores la proximidad del vencimiento de su certificado enviando un correo electrónico antes del vencimiento.
- Cumplir lo dispuesto en las Prácticas de Certificación.
- Disponer de personal calificado, con el conocimiento y la experiencia necesaria para la prestación del servicio de certificación ofrecido por ICERT-EC.
- Aprobar o denegar las solicitudes de emisión de certificados enviadas por la Autoridad de Registro.
- Publicar en la página web de la ICERT-EC la siguiente información:
  a) Las Prácticas de Certificación y todas sus actualizaciones.
  b) Las obligaciones del suscriptor y la forma en que han de custodiarse los datos.
  c) El procedimiento de revocación de su certificado.
  d) Mecanismos para garantizar la fiabilidad de la firma electrónica a lo largo del tiempo.
  e) Las condiciones y límites del uso del certificado.
- Informar a los suscriptores de la revocación de sus certificados inmediatamente de que se produzca dicho evento.
- Informar a la Entidad de Control sobre los eventos que puedan comprometer la prestación del servicio de ICERT-EC.
- Tomar medidas contra la falsificación de certificados y precautelar su confidencialidad durante el proceso de generación y su entrega al suscriptor mediante un procedimiento seguro.

9.6.2. Obligaciones y garantías de la RA

El personal que labora en la RA está obligado a:

- Realizar sus operaciones de acuerdo a esta DPC.
- Respetar y cumplir las disposiciones estipuladas en las Prácticas de Certificación, y en el contrato suscrito con cada suscriptor.
- Exigir al solicitante todos los documentos requeridos para el tipo de certificado que desea obtener.
- Comprobar exhaustivamente la identidad de las personas solicitantes de certificados verificando la exactitud, suficiencia y autenticidad de la información suministrada por el solicitante.

- No almacenar ni copiar los datos de creación de certificado de firma de la persona que haya solicitado sus servicios.
- Proteger los datos de carácter personal suministrados por el solicitante de acuerdo a la política para el manejo de información confidencial.
- Informar antes de la emisión de un certificado, a la persona que solicite sus servicios, de las obligaciones que asume, la forma en que debe custodiar los datos de creación de firma, el procedimiento que debe seguir para comunicar la pérdida o la utilización indebida de los datos o dispositivos de creación y de verificación de firma, de su precio, de las condiciones para la utilización del certificado, de sus limitaciones de uso y de la página web donde puede consultar cualquier información de la ICERT-EC, la DPC y las PC vigentes y anteriores, la legislación aplicable y los procedimientos aplicables para la resolución extrajudicial de los conflictos que pudieran surgir por el ejercicio de la actividad.
- Verificar que el solicitante ha realizado el pago del certificado digital que desea adquirir antes de iniciar el trámite de la emisión del certificado.
- Validar y enviar de forma segura y con la debida celeridad a la CA las solicitudes que reciba para la emisión del certificado y recibir los certificados emitidos.
- Formalizar con el suscriptor los contratos de emisión de certificados en los términos y condiciones que establezca la ICERT-EC y en la Política de Certificados aplicable.
- Hacer entrega del certificado al suscriptor.
- Almacenar de forma segura tanto la documentación entregada por el suscriptor como la generada por la RA durante el proceso de registro o revocación.
- Notificar al solicitante el rechazo de una solicitud de certificación y el motivo que lo causa.
- Precautelar que todos los trámites realizados sean firmados electrónicamente por los operadores que los realizan, asumiendo de esta forma su plena responsabilidad en el proceso.

9.6.3. Obligaciones y garantías de los suscriptores

Son obligaciones de los suscriptores de los certificados emitidos por la ICERT-EC:

- Garantizar la veracidad de la información proporcionada en el momento de solicitar el certificado digital y la información que contiene el certificado.

- Custodiar la clave privada para evitar que otras personas puedan suplantar su identidad y firmar documentos en su nombre o acceder a mensajes confidenciales. La utilización de la clave privada por otras personas es responsabilidad y riesgo del titular del certificado.
- Usar el certificado según lo dispuesto en las políticas de certificado aplicables.
- Respetar las disposiciones del contrato de suscripción y las limitaciones de uso del certificado.
- Utilizar la clave privada únicamente con dispositivos criptográficos acordes a los niveles de seguridad exigidos por la ICERT-EC.
- Informar a la mayor brevedad posible la existencia de alguna causa de revocación.
- Informar cualquier cambio en los datos aportados para la creación del certificado durante su periodo de validez.
- No utilizar la clave privada y el certificado desde el momento en que se solicita su revocación y tampoco cuando el certificado que avala el par de claves no sea válido.
- Verificar que la información contenida en el certificado es verdadera y exacta, en caso de existir algún dato incompleto o incorrecto notificar de inmediato a ICERT-EC.

9.6.4. Obligaciones y garantías de las partes relacionadas

Es obligación de las partes que confían en los certificados emitidos por ICERT-EC:

- Verificar, antes de depositar su confianza en un certificado identificando su validez al momento de efectuar cualquier acción basada en él y asegurarse de que el certificado es apropiado para el uso que se pretende.
- Aceptar que los mensajes o documentos firmados con la clave privada del suscriptor tienen el mismo efecto y validez legal que si se hubiera realizado la firma manuscrita
- Conocer y sujetarse a las garantías, límites y responsabilidades aplicables en la aceptación y uso de los certificados digitales en los que confía.
- Notificar cualquier hecho o situación anómala relativa al certificado y que pueda ser considerada como causa de revocación.

9.7. Exclusión de garantías

ICERT-EC no se hará responsable en las siguientes circunstancias:

- Desastres naturales o cualquier otro caso de fuerza mayor.

- Uso de los certificados siempre y cuando exceda de lo dispuesto en la normativa vigente y la presente DPC, utilizar un certificado revocado o por depositar confianza en él sin antes verificar el estado del mismo.
- Por el uso fraudulento de los certificados o CRL (Lista de Certificados Revocados).
- Por daños y/o perjuicios producto de la errada interpretación de las Prácticas de Certificación por parte de usuarios y suscriptores en el uso de los servicios.
- Por el incumplimiento de las obligaciones establecidas para el suscriptor o usuarios en la normativa vigente.
- Por el contenido de los mensajes o documentos firmados o por el contenido de páginas web que posean un certificado.

- Por prácticas no notificadas a la entidad ICERT-EC que afecten la clave privada del suscriptor permitiendo su uso por terceros (por ejemplo: robo, pérdida o compromiso).
- Por la no recuperación de documentos cifrados con la clave pública del suscriptor.
- Por fraude en la documentación presentada por el solicitante o datos ingresados de forma incorrecta en la solicitud por el operador de la RA.
- Por uso del certificado por parte del suscriptor fuera de su periodo de vigencia o cuando la ICERT-EC haya informado la revocación del certificado.

En el contrato firmado con el suscriptor se obliga al suscriptor a indemnizar a la ICERT-EC como Entidad de Certificación, por cualquier acto u omisión que provoque daños, pérdidas, deudas y gastos procesales en los que esta entidad de certificación pudiera incurrir, que sean causados por la utilización, mal uso, publicación de los certificados proviniendo de:

- Incumplimiento de términos, condiciones y obligaciones establecidos en la Declaración de Prácticas de Certificación.
- Falsedad en los datos suministrados por los suscriptores.
- Omisión en hechos fundamentales que afectan la naturaleza del certificado.
- Incumplimiento en la custodia de claves privadas.

9.8. Limitaciones de responsabilidad

La ICERT-EC responderá por los daños y perjuicios que se causare a cualquier persona, en el ejercicio de su actividad, cuando incumpla las obligaciones previstas en la Ley 2002 - 67 o actúe con negligencia.

La ICERT-EC responderá por los perjuicios que se causaren al firmante o a terceros que confían por la falta o el retraso en la inclusión en el servicio de consulta sobre la vigencia de los certificados, de la extinción o suspensión de la vigencia del certificado emitido por la ICERT-EC, una vez tenga conocimiento de ello.

La ICERT-EC asume toda la responsabilidad frente a terceros por la actuación de las personas que realicen las funciones necesarias para la prestación del servicio de certificación.

La ICERT-EC es una entidad de derecho público. La responsabilidad de la administración se asienta sobre bases objetivas y cubre toda lesión que los particulares sufran siempre que sea consecuencia del funcionamiento anormal de los servicios.

La ICERT-EC sólo responderá por los daños y perjuicios causados por el uso indebido del certificado reconocido, cuando no haya consignado en él, de forma claramente reconocible por terceros, el límite en cuanto a su posible uso. No responderá cuando el suscriptor supere los límites que figuran en el certificado en cuanto a sus posibles usos o no lo utilice conforme a las condiciones establecidas y comunicadas al suscriptor por la ICERT-EC. Tampoco responderá la ICERT-EC si el destinatario de los documentos firmados electrónicamente no comprueba y tiene en cuenta las restricciones que figuran en el certificado en cuanto a sus posibles usos.

9.9. Indemnizaciones

La ICERT-EC incluye en los contratos que la vinculan con el suscriptor las cláusulas de indemnización en caso de incumplimiento de sus obligaciones legales o contractuales.

El suscriptor debe indemnizar a ICERT-EC como Entidad de Certificación por cualquier acto u omisión que provoque daños, pérdidas, deudas y gastos procesales en los que ICERT-EC pudiera incurrir, que sean causados por la utilización, mal uso y publicación de los certificados y que provenga de:

- Incumplimiento de los términos y obligaciones establecidos en la Declaración de Prácticas de Certificación.
- Falsedad en los datos suministrados por los suscriptores.
- Omisión en hechos fundamentales que afectan la naturaleza del certificado.
- Incumplimiento en la custodia de claves privadas.

9.10. Plazo y terminación

La Declaración de Prácticas de Certificación y cada una de las políticas de certificado entran en vigencia desde el momento en que se publican en la página web de la ICERT-EC, a partir de ese momento la versión anterior del documento queda derogada y la nueva versión reemplaza íntegramente la versión anterior. La ICERT-EC conserva en el repositorio las anteriores versiones de la DPC y de cada PC

Para los certificados digitales que hayan sido emitidos bajo una versión antigua de DPC o PC aplica la nueva versión de la DPC o PC en todo lo que no se oponga a las declaraciones de la versión anterior.

9.11. Notificación individual e información a los participantes

Toda notificación, demanda, solicitud o cualquier otra comunicación requerida bajo las prácticas descritas en esta DPC se realizará mediante correos electrónicos, a través de la página web de la ICERT-EC, notas de prensa o cualquier otro mecanismo establecido por la Entidad de Certificación.

9.12. Modificaciones en las DPC y PC

La ICERT-EC puede modificar unilateralmente este documento, sujetándose al siguiente procedimiento:

- La modificación tiene que estar justificada desde el punto de vista técnico y legal.
- La modificación propuesta por la ICERT-EC no puede vulnerar las disposiciones contenidas en las políticas de certificado establecidas por la ICERT-EC.
- Se establece un control de modificaciones, basado en la Política de Gestión de Cambios de la ICERT-EC.
- Se establecen las implicaciones que el cambio de especificaciones tiene sobre el usuario, y se prevé la necesidad de notificarle dichas modificaciones, y esta guarda relación con lo determinado en el numeral 2.2 y 2.3 de este documento.
- Se envía notificación sobre el cambio al organismo de control (ARCOTEL).

9.12.1. Procedimiento de cambio

El procedimiento de cambio será determinado por Subdirección Nacional de Seguridad de la Información, instancia que administra la presente DPC.

9.12.2. Mecanismo y período de notificación

Toda modificación que sufriera este documento de Declaración de Prácticas de Certificación o las Políticas de Certificados se publicará en el sitio web de la ICERT-EC.

9.12.3. Circunstancias bajo las cuales el OID debe cambiarse

Los OID siempre se mantienen y se generan nuevos OID cuando el Consejo de la Judicatura lo considere necesario. No se considera necesario comunicar este tipo de modificaciones a la PC o DPC a los usuarios de los certificados correspondientes a la PC o DPC modificada.

9.13. Prevención y resolución de controversias

Si una controversia entre las partes surge o se relaciona con la presente Declaración de Prácticas de Certificación, el incumplimiento de las estipulaciones en ella contenidas, o cualquier actuación u obligación debida por la presente así como sus contratos adyacentes de existir, considerando que si la controversia no puede ser resuelta a través de negociaciones directas, las partes involucradas acuerdan primero intentar de buena fe resolver la controversia mediante la mediación y el arbitraje de conformidad con las normas y leyes ecuatorianas. El costo de la mediación o arbitraje será absorbido por quien pierda y que conste en el dictamen o laudo arbitral.

9.14. Legislación aplicable

El funcionamiento de la Entidad de Certificación del Consejo de la Judicatura, las operaciones realizadas, la presente Declaración de Prácticas de Certificación, así como las políticas de certificado aplicables a cada tipo de certificado están sujetos a la siguiente normativa:

a) 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. [Ley No. 2002 –67].
b) Reglamento a la Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos (No. 3496) y las Reformas contenidas en los decretos 1356 y 867.
c) Decreto Ejecutivo 908, R.O. 168, 19-XII-2005
d) Resolución 477-20-CONATEL-2008 Modelo de Acreditación como Entidad de
Certificación de Información y Servicios Relacionados
e) Resolución 479-20 CONATEL 2008 Reglamento para la Organización y Funcionamiento del Registro Público Nacional de Entidades de Certificación de

Información y Servicios Relacionados Acreditadas y Terceros Vinculados

f) Acuerdo Ministerial N. 181 – 2011 – Ministerio de Telecomunicaciones y Sociedad de la Información

g) Acuerdo Ministerial No. 12 - 2016 – Ministerio de Telecomunicaciones y Sociedad de la Información

9.15. Cumplimiento de la legislación aplicable

La ICERT-EC declara que la presente DPC cumple con las disposiciones de la legislación aplicable descrita en el apartado anterior.

9.16. Estipulaciones diversas

9.16.1. Cláusula de aceptación completa

Todos los terceros que confían asumen en su totalidad el contenido de la última versión de la DPC y de las PC que sean aplicables.

9.16.2. Independencia

En el caso de que una o más estipulaciones de esta Declaración de Prácticas de Certificación sean o llegasen a ser inválidas, nulas, o inexigibles legalmente, se entenderá por no incluidas, salvo que dichas estipulaciones fueran esenciales de manera que al excluirlas de la DPC careciera ésta, de toda eficacia jurídica.

10. Referencias

La presente Declaración de Prácticas de Certificación (DPC) está fundamentada en las siguientes recomendaciones contenidas en:

[X.509] Norma de la UIT que regula la interconexión de los sistemas de procesamiento de información con el fin de proporcionar servicios de directorio. Para su aplicación en Infraestructura de Clave Pública la norma desarrolla el marco al que deben regirse las Declaraciones de Prácticas de Certificación y las Políticas de Certificado.

[RFC2560] RFC 2560. X.509 Internet Public Key Infrastructure Online Certificate Status Protocol – OCSP. June 1999.

[RFC3161] RFC 3161. Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP). August 2001.

[RFC3628] RFC 3628. Internet X.509 Public Key Infrastructure Time-Stamp Authorities (TSAs). August 2001.

[RFC3629] RFC 3629. UTF-8, a transformation format of ISO 10646. November 2003.

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

[RFC 7382] RFC 7382. Template for a Certification Practice Statement (CPS) for the Resource PKI (RPKI), April 2015.

[CWA14167-1] CWA 14167-1. Security Requirements for Trustworthy Systems Managing Certificates for Electronic Signatures - Part 1: System Security Requirements. June 2003.

[LEY2002-67] Ley No. 2002-67. Ley de comercio electrónico, firmas electrónicas y mensajes de datos.

[LEY2021-459] Ley Orgánica de Protección de Datos Personales, Registro Oficial Suplemento 459 de 26-may.-2021.

[LEY2023-245] Ley Orgánica para la Transformación Digital y Audiovisual, Registro Oficial-Tercer suplemento Nro. 245 de 07 de febrero de 2023.

[DECRETO3496] Decreto No. 3496. Reglamento a la Ley de comercio electrónico, firmas electrónicas y mensajes de datos.

[DECRETO1356] Decreto Nº 1356. Reformas al Reglamento general a la Ley de comercio electrónico, firmas electrónicas y mensajes de datos.

[DECRETO867] Decreto Nº 867. Reforma al Reglamento general a la Ley de comercio electrónico, firmas electrónicas y mensajes de datos. Registro Oficial Nº 532.

[DECRETO-813] Reglamento General a la Ley Orgánica de Transformación Digital y Audiovisual, Segundo suplemento del Registro Oficial 350, 11 de julio de 2023.

[DECRETO-904] Reglamento de la Ley Orgánica de Protección de Datos Personales, 13 de noviembre de 2023.

[MINTEL-181] Ministerio de Telecomunicaciones y de la Sociedad de la Información. Acuerdo Nº 181.

[MINTEL-012] Ministerio de Telecomunicaciones y de la Sociedad de la Información. Acuerdo Nº 12 de 23 de mayo de 2016.

Firmas de Responsabilidad:

	Nombre	Cargo	Firma
Elaborado por:	Cristian Santiago Freire Rodríguez	Supervisor de Seguridad de la Información	Nombre: CRISTIAN SANTIAGO FREIRE RODRIGUEZ Razón: Firma Electrónica Fecha: 23/05/2024 11:15
Revisado por:	Manuel Alejandro Pineda Serrano	Jefe Departamental de Seguridad de la Información	Nombre: MANUEL ALEJANDRO PINEDA SERRANO Razón: Firma Electrónica Fecha: 23/05/2024 11:16
Aprobado por:	Peter Antonio Cabrera Zambrano	Subdirector Nacional de Seguridad de la Información	PETER ANTONIO CABRERA ZAMBRANO Firmado digitalmente por PETER ANTONIO CABRERA ZAMBRANO Fecha: 2024.05.23 11:23:52 -05'00'
Autorizado por:	Hernán Alfonso Calisto Moncayo	Director General	HERNAN ALFONSO CALISTO MONCAYO Firmado digitalmente por HERNAN ALFONSO CALISTO MONCAYO Fecha: 2024.05.23 17:07:10 -05'00'