



**ENTIDAD DE CERTIFICACIÓN DEL CONSEJO DE  
LA JUDICATURA ICERT-EC**

**POLÍTICAS DE CERTIFICADOS**

**Certificado de Miembro de Empresa**

---

**SUBDIRECCIÓN NACIONAL DE SEGURIDAD DE LA  
INFORMACIÓN**

**JEFATURA DE FIRMA ELECTRÓNICA**

**FECHA: 06/05/2024**

	<b>Política de Certificados de Miembro de Empresa</b>			
	<b>CÓDIGO</b>	<b>VERSIÓN</b>	<b>MES Y AÑO</b>	<b>Pág.</b>
	JFE-SNS-2024-016-CF	05	Mayo de 2024	2 de 45

<b>Código:</b>	JFE-SNS-2024-016-CF
<b>Versión:</b>	5.0
<b>Fecha de elaboración</b>	06/05/2024
<b>Elaborado por:</b>	Cristian Freire, Manuel Pineda
<b>Nivel de confidencialidad:</b>	PÚBLICO

### Historial de versiones:

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

	<b>Política de Certificados de Miembro de Empresa</b>			
	CÓDIGO	VERSIÓN	MES Y AÑO	Pág.
	JFE-SNS-2024-016-CF	05	Mayo de 2024	3 de 45

## CONTENIDO

<b>1. INTRODUCCIÓN .....</b>	<b>7</b>
1.1. Presentación general del documento.....	7
1.2. Nombre del documento e identificación.....	8
1.3. Identificación de los tipos de certificado .....	8
1.4. Dispositivos para certificados de miembro de empresa.....	9
1.5. Administración de la Política de Certificados de Miembro de Empresa	9
1.5.1. Entidad que administra el certificado .....	9
1.5.2. Persona de contacto.....	9
1.5.3. Procedimiento para aprobación de la política.....	10
1.5.4. Publicidad .....	10
1.6. Entidades y personas participantes .....	10
1.6.1. Autoridad de Certificación (CA) .....	10
1.6.2. Autoridades de Registro (RA) .....	11
1.6.3. Solicitante .....	11
1.6.4. Suscriptor .....	11
1.6.5. Terceros que confían .....	11
1.7. Ámbito de aplicación de los certificados.....	12
1.7.1. Tiempo de validez de los certificados .....	12
1.7.2. Uso apropiado de los certificados.....	12
1.7.2.1. Autenticación de identidad.....	12
1.7.2.2. Firma digital.....	12
1.7.2.2.1. Autenticidad del origen.....	12
1.7.2.2.2. Integridad del documento .....	12
1.7.2.2.3. No repudio.....	12
1.8. Límites de uso de los certificados.....	13
1.9. Usos prohibidos de los certificados.....	13
1.10. Exención de responsabilidad .....	13
1.11. Definiciones.....	14
1.12. Siglas.....	16
1.13. Referencias a otros documentos .....	17
<b>2. PUBLICACIÓN Y REGISTRO DE CERTIFICADOS .....</b>	<b>18</b>
<b>3. IDENTIFICACIÓN Y AUTENTICACIÓN.....</b>	<b>20</b>
3.1. Registro inicial.....	20
3.2. Nombres .....	20
3.2.1. Tipos de nombres.....	20
3.2.2. Necesidad de que los nombres sean significativos .....	20
3.2.3. Anónimos y seudónimos en los nombres.....	21
3.2.4. Reglas para la interpretación de diversas formas de nombre.....	21

	Política de Certificados de Miembro de Empresa			
	CÓDIGO	VERSIÓN	MES Y AÑO	Pág.
	JFE-SNS-2024-016-CF	05	Mayo de 2024	4 de 45

3.2.5.	Unicidad de los nombres.....	21
3.3.	Validación inicial de la identidad .....	21
3.3.1.	Método para probar la posesión de la clave privada.....	21
3.3.2.	Autenticación de la identidad de miembro de empresa .....	22
3.3.3.	Información de solicitante no verificada.....	23
3.3.4.	Identificación y autenticación para solicitudes de revocación.....	23
<b>4.</b>	<b>REQUISITOS OPERACIONALES PARA EL CICLO DE VIDA DE LOS CERTIFICADOS .....</b>	<b>24</b>
4.1.	Solicitud de certificados.....	24
4.1.1.	Persona apta para presentar una solicitud de certificado.....	24
4.1.2.	Presentación de una solicitud de certificado.....	24
4.1.3.	Comprobación de solicitudes .....	24
4.1.4.	Proceso de solicitud de certificados y responsabilidades de los solicitantes	24
4.1.5.	Aprobación de la solicitud .....	25
4.1.6.	Archivo de la solicitud .....	25
4.1.7.	Registro de pago .....	25
4.2.	Emisión de certificados .....	26
4.2.1.	Acciones de la AC durante la emisión del certificado.....	26
4.2.2.	Notificación al suscriptor por parte de la AC de la emisión del certificado	27
4.3.	Aceptación del certificado .....	27
4.3.1.	Aceptación del certificado por el solicitante .....	27
4.3.2.	Publicación del certificado por la AC.....	27
4.4.	Par de claves y uso del certificado .....	27
4.4.1.	Uso de la clave privada y del certificado por parte del suscriptor .....	27
4.4.2.	Uso de la clave pública y del certificado por los terceros que confían	28
4.5.	Renovación de certificados.....	28
4.5.1.	Razones para la renovación de certificados .....	28
4.6.	Renovación de certificados con cambio de claves .....	28
4.6.1.	Situaciones para la renovación de un certificado con cambio claves.	28
4.6.2.	¿Quién puede pedir la renovación de los certificados? .....	29
4.6.3.	Procesamiento de las solicitudes de renovación de certificados .....	29
4.6.4.	Conducta de aceptación del certificado renovado .....	29
4.7.	Modificación de certificados .....	29
4.7.1.	Circunstancias para la modificación de un certificado .....	29
4.8.	Revocación, suspensión y reactivación de certificados .....	29
4.8.1.	Circunstancias para la revocación.....	30
4.8.2.	Circunstancias para la suspensión.....	31
4.8.3.	Procedimiento para la solicitud de suspensión .....	31
4.8.4.	Plazo límite del tiempo de suspensión.....	31

	<b>Política de Certificados de Miembro de Empresa</b>			
	CÓDIGO	VERSIÓN	MES Y AÑO	Pág.
	JFE-SNS-2024-016-CF	05	Mayo de 2024	5 de 45

4.9.	Servicios de información del estado del certificado .....	31
4.10.	Finalización de la suscripción.....	31
<b>5.</b>	<b>CONTROLES DE SEGURIDAD FÍSICA, INSTALACIONES, GESTIÓN Y OPERACIONALES.....</b>	<b>32</b>
5.1.	Los aspectos referentes a los controles de seguridad: física, de las instalaciones, de personal, auditoría y operacionales definidos para trabajar en un ambiente fiable y seguro, se encuentran especificados en la Declaración de Prácticas de Certificación de la ICERT-EC. ....	32
<b>6.</b>	<b>CONTROLES DE SEGURIDAD TÉCNICA .....</b>	<b>33</b>
6.1.	Generación de claves e instalación.....	33
6.1.1.	Generación del par de claves.....	33
6.1.2.	Entrega de la clave privada al suscriptor.....	33
6.1.3.	Entrega de la clave pública al suscriptor del certificado .....	34
6.1.4.	Disponibilidad de la clave pública.....	34
6.1.5.	Periodo de utilización de la clave privada .....	34
6.1.6.	Tamaño de las claves .....	34
6.1.7.	Parámetros de generación de la clave pública y verificación de la calidad	34
6.1.8.	Fines de uso de la clave X.509 v3.....	34
6.2.	Controles sobre la clave privada del suscriptor.....	34
6.2.1.	Estándares para los módulos criptográficos .....	36
6.2.2.	Control multipersona de la clave privada .....	36
6.2.3.	Custodia de la clave privada .....	36
6.2.4.	Copia de seguridad de la clave privada.....	36
6.2.5.	Archivo de la clave privada.....	36
6.2.6.	Transferencia de la clave privada a o desde el módulo criptográfico .	37
6.2.7.	Almacenamiento de la clave privada en un módulo criptográfico .....	37
6.2.8.	Método de activación de la clave privada .....	37
6.2.9.	Método de desactivación de la clave privada .....	37
6.2.10.	Método de destrucción de la clave privada.....	38
6.2.11.	Clasificación de los módulos criptográficos .....	38
6.3.	Otros aspectos de la administración del par de claves.....	38
6.3.1.	Archivo de la clave pública .....	38
6.3.2.	Periodos operacionales del certificado y periodos de uso del par de claves	38
6.3.3.	Datos de activación.....	38
6.3.4.	Generación de datos de activación e instalación.....	38
6.3.5.	Protección de datos de activación.....	39
6.4.	Controles de seguridad informática.....	39
<b>7.</b>	<b>PERFILES DE CERTIFICADO, CRL Y OCSP .....</b>	<b>39</b>
7.1.	Contenido del certificado.....	40
7.2.	Número de versión.....	41

	Política de Certificados de Miembro de Empresa			
	CÓDIGO	VERSIÓN	MES Y AÑO	Pág.
	JFE-SNS-2024-016-CF	05	Mayo de 2024	6 de 45

Extensiones del certificado .....	41
7.2.1 Identificadores de objeto de los algoritmos.....	42
7.2.2 Formatos de nombre .....	42
7.2.3 Restricciones de nombre .....	43
7.2.4 Objeto identificador de la Política de Certificados .....	43
7.2.5 Sintaxis y semántica de los calificadores de la política.....	43
7.3 Perfil de la CRL.....	43
7.3.1 Número de versión.....	43
7.3.2 CRL y extensiones .....	43
7.3.3 Perfil OCSP .....	43
7.3.4 Numero de versión.....	43
7.3.5 Extensiones OCSP .....	43
<b>8. AUDITORIA DE CONFORMIDAD Y OTRAS VALORACIONES .....</b>	<b>43</b>
<b>9. OTROS NEGOCIOS Y ASUNTOS LEGALES.....</b>	<b>44</b>
9 Tarifas.....	44
9.1 Responsabilidad financiera.....	44
9.2 Confidencialidad de la información .....	44
9.3 Protección de la información personal.....	44
9.4 Derechos de propiedad intelectual.....	44
9.5 Obligaciones y garantías.....	44
9.6 Limitaciones de responsabilidad.....	44
9.7 Indemnizaciones.....	44
9.8 Duración y terminación.....	44
9.9 Procedimiento de cambio en las especificaciones .....	44
9.10 Prevención de disputas .....	44
9.11 Ley aplicable .....	44
9.12 Estipulaciones diversas.....	45
9.12.1 Cláusula de aceptación completa.....	45
9.12.2 Independencia .....	45

	<b>Política de Certificados de Miembro de Empresa</b>			
	CÓDIGO	VERSIÓN	MES Y AÑO	Pág.
	JFE-SNS-2024-016-CF	05	Mayo de 2024	7 de 45

## 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 realizar la emisión de certificados electrónicos para toda la Función Judicial; implementó la Infraestructura de Clave Pública (PKI).

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

*“Artículo 1.- Sustituir el undécimo artículo innumerado agregado a continuación del artículo 17, referente a la Acreditación para Entidades del Estado, con el siguiente texto:*

*Acreditación para Entidades del Estado. - Las instituciones y entidades del Estado, así como las empresas públicas, señaladas en la Constitución de la República, de acuerdo con la Disposición General Octava de la Ley, podrán prestar servicios como Entidades de Certificación de Información y Servicios Relacionados, previa resolución emitida por el CONATEL.*

*Las instituciones públicas obtendrán certificados de firma electrónica de las Entidades de Certificación de Información y Servicios Relacionados Acreditadas, de derecho público o de derecho privado.”*

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

### 1.1. Presentación general del documento

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

Los certificados de miembro de empresa son certificados que identifican al suscriptor como una persona física que presta sus servicios lícitos y personales

	Política de Certificados de Miembro de Empresa			
	CÓDIGO	VERSIÓN	MES Y AÑO	Pág.
	JFE-SNS-2024-016-CF	05	Mayo de 2024	8 de 45

en una empresa, la cual autoriza al suscriptor obtener un certificado de firma electrónica. Los miembros de empresa serán responsables en tal calidad, de todo lo que firmen dentro del ámbito de su competencia y límites de uso que correspondan.

## 1.2. Nombre del documento e identificación

Este documento se denomina Política de Certificados de Miembro de Empresa, el cual contiene la siguiente información que podrá ser consultada en la página web [www.icert.fje.gob.ec](http://www.icert.fje.gob.ec) en la ubicación:

[http://www.icert.fje.gob.ec/dpc/pc\\_miembro\\_empresa.pdf](http://www.icert.fje.gob.ec/dpc/pc_miembro_empresa.pdf).

Nombre del documento	<b>POLÍTICA DE CERTIFICADOS</b> <b>Certificados de miembro de empresa</b>
Descripción	<i>Los certificados de miembro de empresa acreditan la identidad del suscriptor y le permiten firmar documentos electrónicamente con la misma validez legal que la firma manuscrita.</i>
Identificador OID	1.3.6.1.4.1.43745.1.2.1.4
Versión	5.0
Fecha de emisión	06 de mayo de 2024
Ubicación	<a href="http://www.icert.fje.gob.ec/dpc/pc_miembro_empresa.pdf">http://www.icert.fje.gob.ec/dpc/pc_miembro_empresa.pdf</a>

## 1.3. Identificación de los tipos de certificado

Cada tipo de certificado recibe su propio OID, indicado e incluido dentro del certificado, en el campo identificador OID. Cada OID es particular y no se emplea para identificar diferentes tipos, políticas y versiones de los certificados emitidos. Los certificados de miembro de empresa emitidos por la ICERT-EC tienen asignados los siguientes identificadores de objeto (OID) dependiendo del tipo de contenedor criptográfico:

<b>1.3.6.1.4.1.43745.1.2.1.4</b>	<b>Certificado de Miembro de Empresa</b>
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)

	<b>Política de Certificados de Miembro de Empresa</b>			
	CÓDIGO	VERSIÓN	MES Y AÑO	Pág.
	JFE-SNS-2024-016-CF	05	Mayo de 2024	9 de 45

#### 1.4. Dispositivos para certificados de miembro de empresa

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

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

#### 1.5. Administración de la Política de Certificados de Miembro de Empresa

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

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

##### 1.5.1. Entidad que administra el certificado

<b>ENTIDAD DE CERTIFICACIÓN</b>	ENTIDAD DE CERTIFICACION ICERT - EC
<b>NOMBRE</b>	Subdirección Nacional de Seguridad de la Información
<b>DIRECCIÓN</b>	Av. 12 de octubre N24-593 y Francisco Salazar
<b>TELÉFONO</b>	(02) 395 3600
<b>Email</b>	<a href="mailto:entidad.certificacion@funcionjudicial.gob.ec">entidad.certificacion@funcionjudicial.gob.ec</a>

##### 1.5.2. Persona de contacto

<b>ENTIDAD DE CERTIFICACIÓN</b>	ENTIDAD DE CERTIFICACION ICERT - EC
<b>NOMBRE</b>	Ing. Peter Cabrera Subdirector Nacional de Seguridad de la Información
<b>DIRECCIÓN</b>	Av. 12 de octubre N24-593 y Francisco Salazar
<b>TELÉFONO</b>	+593 2 395 3600

	<b>Política de Certificados de Miembro de Empresa</b>			
	CÓDIGO	VERSIÓN	MES Y AÑO	Pág.
	JFE-SNS-2024-016-CF	05	Mayo de 2024	10 de 45

<b>Email</b>	<a href="mailto:entidad.certificacion@funcionjudicial.gob.ec">entidad.certificacion@funcionjudicial.gob.ec</a>
--------------	--

### 1.5.3. Procedimiento para aprobación de la política

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

### 1.5.4. Publicidad

La Política de Certificados de Miembro de Empresa es un documento público que se encuentra disponible en la página web [http://www.icert.fje.gob.ec/dpc/pc\\_miembro\\_empresa.pdf](http://www.icert.fje.gob.ec/dpc/pc_miembro_empresa.pdf) de la ICERT-EC. Las modificaciones a esta política, que fueren aprobadas de acuerdo con el procedimiento previsto se publicarán de forma inmediata.

## 1.6. Entidades y personas participantes

Los certificados de miembro de empresa son emitidos a las personas físicas que acreditan su condición de pertenencia, función o empleo en una empresa y documentan su identidad como titulares en la firma de documentos electrónicos, garantizando la legitimidad del emisor de la comunicación y la integridad del contenido. El poseedor de un certificado de miembro de empresa interviene con voluntad en nombre de quien representa e interés propio.

### 1.6.1. Autoridad de Certificación (CA)

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

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

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

**CA Raíz:** Autoridad de Certificación de primer nivel. Esta CA sólo emite certificados para sí misma y sus CA Subordinadas. Únicamente estará en funcionamiento durante la generación del certificado auto firmado; de certificados

	<b>Política de Certificados de Miembro de Empresa</b>			
	CÓDIGO	VERSIÓN	MES Y AÑO	Pág.
	JFE-SNS-2024-016-CF	05	Mayo de 2024	11 de 45

de CA subordinada y periódicamente para la generación de la lista de certificados revocados de Autoridad de Certificación Raíz ARL o LRA.

**CA Subordinada:** Autoridad de Certificación Subordinada de CA Raíz. Su función es la emisión de certificados de usuario final, de entre otros, certificados de miembro de empresa.

### 1.6.2. Autoridades de Registro (RA)

Las Autoridades de Registro son las entidades delegadas por la Autoridad de Certificación para la identificación y autenticación de los solicitantes de certificados con el fin de receptar y procesar solicitudes de certificados digitales requiriendo la emisión de los certificados a la CA Subordinada.

Están facultadas, además, para solicitar a la CA Subordinada la revocación, suspensión y reactivación los certificados emitidos por la CA Subordinada.

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

Los tipos de certificados que emite la ICERT-EC serán para uso de cualquier miembro de empresa.

Las Autoridades de Registro llevarán un registro completo de los solicitantes que deseen adquirir un certificado.

### 1.6.3. Solicitante

El solicitante es aquella persona física que a nombre propio y con autorización legal de la empresa, desea acceder a los servicios de certificación digital al adquirir un certificado de miembro de empresa emitido por la ICERT-EC.

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

### 1.6.4. Suscriptor

El suscriptor es aquella persona física a quien se le otorga un certificado de miembro de empresa emitido por la ICERT-EC y se considera suscriptor mientras dicho certificado se encuentre vigente.

### 1.6.5. Terceros que confían

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

	<b>Política de Certificados de Miembro de Empresa</b>			
	CÓDIGO	VERSIÓN	MES Y AÑO	Pág.
	JFE-SNS-2024-016-CF	05	Mayo de 2024	12 de 45

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

## **1.7. Ámbito de aplicación de los certificados**

### **1.7.1. Tiempo de validez de los certificados**

Los certificados digitales de miembro de empresa tendrán una validez de dos (2) años.

### **1.7.2. Uso apropiado de los certificados**

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:

#### **1.7.2.1. 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.

#### **1.7.2.2. 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.

##### **1.7.2.2.1. Autenticidad del origen**

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

##### **1.7.2.2.2. Integridad del documento**

La utilización del certificado garantiza que el documento es 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.

##### **1.7.2.2.3. No repudio**

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

	<b>Política de Certificados de Miembro de Empresa</b>			
	CÓDIGO	VERSIÓN	MES Y AÑO	Pág.
	JFE-SNS-2024-016-CF	05	Mayo de 2024	13 de 45

### 1.8. Límites de uso de los certificados

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

### 1.9. Usos prohibidos de los certificados

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

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

### 1.10. Exención de responsabilidad

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

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

	<b>Política de Certificados de Miembro de Empresa</b>			
	CÓDIGO	VERSIÓN	MES Y AÑO	Pág.
	JFE-SNS-2024-016-CF	05	Mayo de 2024	14 de 45

### 1.11. Definiciones

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

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

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

**Autoridad de Certificación (Certification Authority, 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 receptor 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 AC Subordinada que contiene la lista de todos los certificados de AC Subordinada emitidos por la AC Raíz que hayan sido revocados o suspendidos y que aún no hayan expirado.

**CRL (Certificate Revocation List, 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 AC, se incluye en el certificado digital.

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

	<b>Política de Certificados de Miembro de Empresa</b>			
	CÓDIGO	VERSIÓN	MES Y AÑO	Pág.
	JFE-SNS-2024-016-CF	05	Mayo de 2024	15 de 45

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

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

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

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

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

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

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

	<b>Política de Certificados de Miembro de Empresa</b>			
	<b>CÓDIGO</b>	<b>VERSIÓN</b>	<b>MES Y AÑO</b>	<b>Pág.</b>
	JFE-SNS-2024-016-CF	05	Mayo de 2024	16 de 45

**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)*.

**X.509:** Estándar desarrollado por la UIT-T para infraestructuras de claves públicas que especifica entre otros temas, los formatos estándar para certificados de claves públicas y para la implementación de listas de certificados en revocación.

## 1.12. Siglas

Siglas	Palabras abreviadas
<b>ARL</b>	Authority Revocation List (Lista de revocación de autoridad)
<b>VA</b>	Validation Authority (Autoridad de Validación)
<b>C</b>	Country Name (Nombre del País)
<b>CA</b>	Certification Authority (Autoridad de Certificación)
<b>CJ</b>	Consejo de la Judicatura
<b>CN</b>	Common Name (Nombre común)
<b>cps</b>	certificate practice statement
<b>CRL</b>	Certificate Revocation List (Lista de certificados revocados)
<b>DN</b>	Distinguished Name (Nombre distintivo)
<b>DPC</b>	Declaración de Prácticas de Certificación
<b>DNTICs</b>	Dirección Nacional de Tecnologías de la Información y Comunicaciones
<b>ERC</b>	Emergency Revocation Code (Código de revocación emergente)
<b>HSM</b>	Hardware Security Module (Módulo de Seguridad Criptográfica)
<b>HTTP</b>	Hypertext Transfer Protocol
<b>HTTPS</b>	HTTP Secure
<b>ICERT-EC</b>	Entidad de Certificación del Consejo de la Judicatura
<b>IP</b>	Internet Protocol (Protocolo Internet)

	<b>Política de Certificados de Miembro de Empresa</b>			
	CÓDIGO	VERSIÓN	MES Y AÑO	Pág.
	JFE-SNS-2024-016-CF	05	Mayo de 2024	17 de 45

<b>ISO</b>	International Organization for Standardization (Organismo internacional de estandarización)
<b>L</b>	LocalityName
<b>NIST</b>	National Institute of Standards and Technology
<b>O</b>	OrganizationName
<b>OCSP</b>	Online Certificate Status Protocol (Protocolo de estatus de certificados en línea)
<b>OID</b>	Object Identifier (Identificador de Objetos)
<b>OU</b>	Organizational UnitName
<b>PC</b>	Política de Certificados
<b>PDF</b>	Portable Document Format
<b>PDF/A</b>	PDF/Archive
<b>PIN</b>	Personal Identification Number (Número de identificación personal)
<b>PKCS</b>	Public-Key Cryptography Standard (Estándares de criptografía de clave pública)
<b>PKI</b>	Public Key Infrastructure (Infraestructura de Clave Pública)
<b>PUK</b>	Personal Unlok Key (Clave personal de desbloqueo)
<b>RA</b>	Registration Authority (Autoridad de registro)
<b>RFC</b>	Request For Comments (Petición de comentarios)
<b>RSA</b>	Rivest Shamir Adleman
<b>RUC</b>	Registro Único de Contribuyentes
<b>SFC</b>	Servidor de Firma Centralizada
<b>SHA</b>	Secure Hash Algorithm
<b>SW</b>	Software
<b>TSP</b>	Time-Stamp Protocol (Protocolo de estampado de tiempo)
<b>URL</b>	Uniform Resource Locator
<b>UTC</b>	Universal Time Coordinated
<b>UTF-8</b>	8-bit Unicode Transformation Format
<b>v</b>	version
<b>VA</b>	Validation Authority (Autoridad de validación)

### 1.13. Referencias a otros documentos

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

	Política de Certificados de Miembro de Empresa			
	CÓDIGO	VERSIÓN	MES Y AÑO	Pág.
	JFE-SNS-2024-016-CF	05	Mayo de 2024	18 de 45

- [LEY2002-67]** Ley No. 2002-67. Ley de comercio electrónico, firmas electrónicas y mensajes de datos. Dada en la ciudad de San Francisco de Quito, Distrito Metropolitano, en la sala de sesiones del Pleno del Congreso Nacional del Ecuador, a 10 de abril del 2002.
- [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.
- [DECRETO-3496]** Decreto No. 3496. Reglamento a la Ley de comercio electrónico, firmas electrónicas y mensajes de datos. Dado en el Palacio Nacional, en Quito, a 12 de diciembre del 2002.
- [DECRETO-1356]** Decreto N° 1356. Reformas al Reglamento general a la Ley de comercio electrónico, firmas electrónicas y mensajes de datos. Dado en el Palacio Nacional, en San Francisco de Quito, el día de 29 de septiembre de 2008.
- [DECRETO-867]** Decreto N° 867. Reforma al Reglamento general a la Ley de comercio electrónico, firmas electrónicas y mensajes de datos. Registro Oficial N° 532. Quito, Lunes 12 de Septiembre del 2011.
- [MINTEL-181]** Ministerio de Telecomunicaciones y de la Sociedad de la Información. Acuerdo N° 181. Dado en Quito, Distrito Metropolitano, a 15 de septiembre de 2011.
- [MINTEL-012]** Ministerio de Telecomunicaciones y de la Sociedad de la Información. Acuerdo N° 012-2016. Dado en Quito, Distrito Metropolitano, a 23 de mayo de 2016.

## 2. PUBLICACIÓN Y REGISTRO DE CERTIFICADOS

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

Cualquier cambio o modificación en la Política de Certificados de Miembro de Empresa 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.

	<b>Política de Certificados de Miembro de Empresa</b>			
	CÓDIGO	VERSIÓN	MES Y AÑO	Pág.
	JFE-SNS-2024-016-CF	05	Mayo de 2024	19 de 45

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

	<b>Política de Certificados de Miembro de Empresa</b>			
	<b>CÓDIGO</b>	<b>VERSIÓN</b>	<b>MES Y AÑO</b>	<b>Pág.</b>
	JFE-SNS-2024-016-CF	05	Mayo de 2024	20 de 45

### 3. IDENTIFICACIÓN Y AUTENTICACIÓN

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

#### 3.1. Registro inicial

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

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

#### 3.2. Nombres

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

##### 3.2.1. Tipos de nombres

Todos los certificados de 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	<u>País</u>	Abreviatura del país donde reside el suscriptor
L	<u>Ciudad</u>	Abreviatura de la ciudad donde reside el suscriptor
SerialNumber	<u>Número Serial</u>	Número del documento identificación de miembro de empresa
CN	<u>Nombre común</u>	Nombres y apellidos completos del suscriptor

##### 3.2.2. Necesidad de que los nombres sean significativos

Todo certificado de miembro de empresa emitido por la ICERT-EC tiene como característica principal la plena identificación del suscriptor y la asignación de un nombre significativo a su certificado con la finalidad de vincular la clave pública con su identidad.

	<b>Política de Certificados de Miembro de Empresa</b>			
	CÓDIGO	VERSIÓN	MES Y AÑO	Pág.
	JFE-SNS-2024-016-CF	05	Mayo de 2024	21 de 45

### 3.2.3. Anónimos y seudónimos en los nombres

De acuerdo con esta Política de Certificados no se admiten anónimos ni seudónimos para identificar el nombre de un miembro de empresa.

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

### 3.2.4. Reglas para la interpretación de diversas formas de nombre

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

Todos los nombres de miembros de empresa están escritos utilizando lenguaje natural, prescindiendo de acentos. En ningún caso se pueden modificar los nombres y apellidos de un miembro de empresa, excepto para adaptarlos al formato y longitud del componente *Common Name* en el que se insertan.

### 3.2.5. Unicidad de los nombres

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

## 3.3. Validación inicial de la identidad

### 3.3.1. Método para probar la posesión de la clave privada

Las claves del certificado de miembro de empresa son generadas aleatoriamente. Para demostrar que el titular posee la clave privada correspondiente a la clave pública que se pretende vincular al certificado de miembro de empresa, se probará mediante el envío de la petición de certificado, en la cual se incluirá la clave pública firmada mediante la clave privada asociada.

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

- a) Generación en token o tarjeta criptográfica.

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

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

	<b>Política de Certificados de Miembro de Empresa</b>			
	<b>CÓDIGO</b>	<b>VERSIÓN</b>	<b>MES Y AÑO</b>	<b>Pág.</b>
	JFE-SNS-2024-016-CF	05	Mayo de 2024	22 de 45

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

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

b) Generación y construcción de un PKCS#12 descargable

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

c) Generación en HSM SFC y custodia segura remota

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

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

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

### 3.3.2. Autenticación de la identidad de miembro de empresa

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

NUMERO IDENTIFICADOR	CAMPOS
3.10	<i>Razón social de la empresa</i>
3.11	<i>RUC</i>
3.1	<i>Cédula o pasaporte</i>

	<b>Política de Certificados de Miembro de Empresa</b>			
	CÓDIGO	VERSIÓN	MES Y AÑO	Pág.
	JFE-SNS-2024-016-CF	05	Mayo de 2024	23 de 45

<b>3.2</b>	<b><i>Nombres del suscriptor</i></b>
<b>3.3</b>	<b><i>Primer apellido</i></b>
<b>3.4</b>	<b><i>Segundo apellido</i></b>
<b>3.5</b>	<b><i>Cargo</i></b>
<b>3.7</b>	<b><i>Dirección</i></b>
<b>3.8</b>	<b><i>Teléfono</i></b>
<b>3.9</b>	<b><i>Ciudad</i></b>
<b>3.12</b>	<b><i>País</i></b>

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.

### **3.3.3. Información de solicitante no verificada**

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

### **3.3.4. Identificación y autenticación para solicitudes de revocación**

El procedimiento para identificación y autenticación para generar la solicitud de revocación de un certificado requiere de la autenticación del suscriptor con sus credenciales, que consisten en el identificador unívoco de la solicitud y en el código de emergencia asociado ERC.

También puede ser procesada mediante una solicitud enviada por un tercero debidamente identificado que represente al suscriptor. Asimismo, también es posible mediante una comparecencia física, por la que el operador de validación procederá a la revocación.

	<b>Política de Certificados de Miembro de Empresa</b>			
	CÓDIGO	VERSIÓN	MES Y AÑO	Pág.
	JFE-SNS-2024-016-CF	05	Mayo de 2024	24 de 45

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

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

### 4.1. Solicitud de certificados

#### 4.1.1. Persona apta para presentar una solicitud de certificado

La solicitud de un certificado de miembro de empresa la puede realizar cualquier persona mayor de edad que demuestre estar vinculada laboralmente a una empresa, que se encuentre autorizada por la empresa para actuar en nombre de esta en función del cargo que representa, y que esté en plena capacidad para contratar y obligarse de cumplir con las responsabilidades inherentes al uso de este tipo de certificado.

#### 4.1.2. Presentación de una solicitud de certificado

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

#### 4.1.3. Comprobación de solicitudes

El operador de validación de la ICERT-EC deberá comprobar y validar la información y los documentos que son requeridos para solicitar los certificados de miembro de empresa.

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

Las Autoridades de Registro de la ICERT-EC mantendrán un archivo con la información que respalde cada solicitud realizada para la emisión de los certificados de miembro de empresa, por un período de mínimo cinco (5) años.

#### 4.1.4. Proceso de solicitud de certificados y responsabilidades de los solicitantes

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

	<b>Política de Certificados de Miembro de Empresa</b>			
	<b>CÓDIGO</b>	<b>VERSIÓN</b>	<b>MES Y AÑO</b>	<b>Pág.</b>
	JFE-SNS-2024-016-CF	05	Mayo de 2024	25 de 45

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

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

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

#### **4.1.5. Aprobación de la solicitud**

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

#### **4.1.6. Archivo de la solicitud**

Se rechazarán notificando la causa las solicitudes que no cumplan con los requerimientos, información y documentación solicitada en la presente Política de Certificados de Miembro de Empresa, o que los documentos presentados no sean concordantes. El archivo de la solicitud rechazada da lugar a que el solicitante pueda nuevamente iniciar el proceso de solicitud de certificado. Las solicitudes que hayan sido aprobadas y que no se ha realizado el registro de pago en los treinta (30) días posteriores a su aprobación serán archivadas.

#### **4.1.7. Registro de pago**

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

	<b>Política de Certificados de Miembro de Empresa</b>			
	<b>CÓDIGO</b>	<b>VERSIÓN</b>	<b>MES Y AÑO</b>	<b>Pág.</b>
	JFE-SNS-2024-016-CF	05	Mayo de 2024	26 de 45

## 4.2. Emisión de certificados

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

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

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

No.	Responsable	Descripción de la actividad	Documentos de apoyo
1	Operador de emisión	Revisa que no haya caducado el pago para el certificado a emitir	
2	Operador de emisión	Valida la información que se ingresó mediante solicitud	Documentos escaneados
No.	Responsable	Descripción de la actividad	Documentos de apoyo
3	Usuario suscriptor	Entrega documentos de identidad y presenta comprobante de pago y factura	Comprobante de pago y factura
4	Operador de emisión	Genera el certificado de acuerdo con contenedor solicitado, toma fotografía y genera el contrato. Se envía el sobre de credenciales al usuario	Contrato, correo electrónico con códigos
5	Usuario suscriptor	El usuario firma el contrato	Contrato firmado
6	Operador de emisión	Almacena el contrato y lo envía vía correo	Contrato firmado

### 4.2.1. Acciones de la AC durante la emisión del certificado

Con la emisión del certificado por parte de la AC de la ICERT-EC se perfecciona la aprobación definitiva de la solicitud realizada por parte del miembro de empresa.

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

	Política de Certificados de Miembro de Empresa			
	CÓDIGO	VERSIÓN	MES Y AÑO	Pág.
	JFE-SNS-2024-016-CF	05	Mayo de 2024	27 de 45

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

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

#### 4.3. Aceptación del certificado

##### 4.3.1. Aceptación del certificado por el solicitante

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

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 se considerará la aceptación de éste. Un suscriptor puede enviar un mensaje de no aceptación del certificado incluyendo el motivo del rechazo y la identificación de los motivos, o de ser el caso los campos en el certificado que están incorrectos o incompletos.

##### 4.3.2. Publicación del certificado por la AC

Emitido el certificado de miembro de empresa por parte de la ICERT-EC, se procede a la publicación en el directorio de certificados. La clave pública del certificado es publicada en el correspondiente repositorio de base de datos de la RA.

#### 4.4. Par de claves y uso del certificado

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

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

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

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

	<b>Política de Certificados de Miembro de Empresa</b>			
	CÓDIGO	VERSIÓN	MES Y AÑO	Pág.
	JFE-SNS-2024-016-CF	05	Mayo de 2024	28 de 45

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

Los terceros que confían en los servicios de certificación de la ICERT-EC solo pueden depositar su confianza en los certificados de funciones que requieran acreditar la identidad del titular como miembro de empresa, de conformidad con lo establecido en el campo “keyUsage” del certificado o en la presente Política de Certificados.

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

#### **4.5. Renovación de certificados**

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

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

##### **4.5.1. Razones para la renovación de certificados**

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

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

#### **4.6. Renovación de certificados con cambio de claves**

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

##### **4.6.1. Situaciones para la renovación de un certificado con cambio claves**

Circunstancias por las que se puede renovar un certificado:

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

	<b>Política de Certificados de Miembro de Empresa</b>			
	CÓDIGO	VERSIÓN	MES Y AÑO	Pág.
	JFE-SNS-2024-016-CF	05	Mayo de 2024	29 de 45

#### **4.6.2. ¿Quién puede pedir la renovación de los certificados?**

La renovación de los certificados de miembro de empresa únicamente puede ser solicitada por sus titulares previo a su expiración.

#### **4.6.3. Procesamiento de las solicitudes de renovación de certificados**

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

Las renovaciones de certificados de miembro de empresa están sujetas a las siguientes condiciones:

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

#### **4.6.4. Conducta de aceptación del certificado renovado**

Se establecen las mismas condiciones de aceptación que se determinan en la emisión inicial de certificados de miembro de empresa.

### **4.7. Modificación de certificados**

#### **4.7.1. Circunstancias para la modificación de un certificado**

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

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

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

### **4.8. Revocación, suspensión y reactivación de certificados**

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

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

	<b>Política de Certificados de Miembro de Empresa</b>			
	CÓDIGO	VERSIÓN	MES Y AÑO	Pág.
	JFE-SNS-2024-016-CF	05	Mayo de 2024	30 de 45

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

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

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

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

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

Los certificados suspendidos podrán volver al estado activo.

#### **4.8.1. Circunstancias para la revocación**

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

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

	<b>Política de Certificados de Miembro de Empresa</b>			
	CÓDIGO	VERSIÓN	MES Y AÑO	Pág.
	JFE-SNS-2024-016-CF	05	Mayo de 2024	31 de 45

#### **4.8.2. Circunstancias para la suspensión**

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

Las circunstancias para la suspensión de un certificado son:

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

#### **4.8.3. Procedimiento para la solicitud de suspensión**

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

#### **4.8.4. Plazo límite del tiempo de suspensión**

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

#### **4.9. Servicios de información del estado del certificado**

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

#### **4.10. Finalización de la suscripción**

En el certificado de miembro de empresa se especifica el tiempo de su validez plena y legal, ya que se determina desde y hasta cuando está vigente.

	<b>Política de Certificados de Miembro de Empresa</b>			
	CÓDIGO	VERSIÓN	MES Y AÑO	Pág.
	JFE-SNS-2024-016-CF	05	Mayo de 2024	32 de 45

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

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

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.

	<b>Política de Certificados de Miembro de Empresa</b>			
	CÓDIGO	VERSIÓN	MES Y AÑO	Pág.
	JFE-SNS-2024-016-CF	05	Mayo de 2024	33 de 45

## 6. CONTROLES DE SEGURIDAD TÉCNICA

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

### 6.1. Generación de claves e instalación

#### 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 genera 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 con la forma de entrega del certificado elegido por el suscriptor:

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

#### 6.1.2. Entrega de la clave privada al suscriptor

Para el certificado digital que se emite en dispositivo token/tarjeta criptográfica, la clave privada se genera al realizar el operador de la AR el enrolamiento bajo la presencia del suscriptor, y su uso es protegido mediante un PIN.

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

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

	<b>Política de Certificados de Miembro de Empresa</b>			
	CÓDIGO	VERSIÓN	MES Y AÑO	Pág.
	JFE-SNS-2024-016-CF	05	Mayo de 2024	34 de 45

### **6.1.3. Entrega de la clave pública al suscriptor del certificado**

El mecanismo de entrega de la clave pública a titulares de certificados de miembro de empresa varía si la forma de entrega es en dispositivo token/tarjeta criptográfica, en archivo con formato PKCS#12 o en HSM SFC.

La clave pública de los certificados de miembro de empresa se genera en el dispositivo criptográfico del titular en el puesto de emisión siendo la AR la responsable de entregar dicha clave pública a la AC.

### **6.1.4. Disponibilidad de la clave pública**

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

### **6.1.5. Periodo de utilización de la clave privada**

El periodo de utilización de la clave privada es el mismo tiempo de la vigencia del certificado de miembro de empresa o inferior cuando el certificado es revocado antes de caducar.

### **6.1.6. Tamaño de las claves**

El tamaño de las claves de certificados de miembro de empresa es de 2048 bits.

### **6.1.7. Parámetros de generación de la clave pública y verificación de la calidad**

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

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

### **6.1.8. Fines de uso de la clave X.509 v3**

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

## **6.2. Controles sobre la clave privada del suscriptor**

En el cuadro siguiente se especifican los controles de protección de la clave privada del suscriptor según la forma de entrega del certificado. La protección de los datos de activación es responsabilidad exclusiva del suscriptor.

	<b>Política de Certificados de Miembro de Empresa</b>			
	<b>CÓDIGO</b>	<b>VERSIÓN</b>	<b>MES Y AÑO</b>	<b>Pág.</b>
	JFE-SNS-2024-016-CF	05	Mayo de 2024	35 de 45

Control de la ICERT-EC para protección de la clave privada	Forma de entrega del certificado		
	Dispositivo token	Archivo PKCS #12	HSM SFC
<b>Respaldo de la clave privada</b>	ICERT-EC no realiza respaldo sobre las claves privadas de los suscriptores generadas desde dispositivo token. ICERT-EC nunca está en posesión de dichas claves y solo permanecen bajo custodia del propio suscriptor.	ICERT-EC no realiza respaldo de los archivos PKCS#12 ni de la clave privada en él contenida. Una vez generado es enviado al suscriptor.	ICERT-EC no realiza respaldo legible o que pueda utilizarse sin las credenciales del usuario de las claves privadas de los suscriptores generadas en HSM y custodiadas de manera segura.  La clave privada es única y es cifrada/descifrada por una clave sólo conocida y custodiada en el HSM. Sólo el suscriptor dispone de los mecanismos para su uso.
<b>Almacenamiento de la clave privada</b>	Las claves privadas de los suscriptores generadas en dispositivo token o tarjeta criptográfica NUNCA son almacenadas por ICERT-EC.  La clave privada debe ser almacenada por el propio suscriptor mediante la conservación del dispositivo token o por otros métodos, debido a que puede ser necesaria para descifrar la información histórica cifrada con la clave pública.	Las claves privadas de los suscriptores contenidas en archivos PKCS #12 NUNCA son almacenadas por ICERT-EC.  El archivo PKCS #12 se envía al suscriptor para que éste lo almacene y conserve.	Las claves privadas de los suscriptores generadas en HSM son almacenadas en una base de datos del SFC en un blob cifrado mediante una clave solamente conocida por el HSM y activable sólo por el suscriptor.  Para utilizar la clave privada del suscriptor es necesario descifrarla mediante una autenticación utilizando credenciales que sólo el suscriptor posee.
<b>Transferencia de la clave privada</b>	La clave privada de los suscriptores generada en token/tarjeta criptográfica nunca sale del propio dispositivo/contenedor.  Con el dispositivo token/tarjeta criptográfica se genera el par de claves y se protege su uso a través de un PIN que solo conoce el suscriptor.	La clave privada de los suscriptores se encuentra dentro del archivo PKCS #12, el cual se envía por correo electrónico al suscriptor. En un correo electrónico adicional se envía la contraseña de dicho PKCS#12.  El archivo PKCS #12 protege el uso de la clave privada a través de una clave que es custodiada por el suscriptor.	La clave privada de los suscriptores generada en el HSM nunca sale descifrada del propio HSM.  Siempre que la clave privada viaja fuera del HSM está cifrada, y sólo el HSM puede descifrarla mediante credenciales que sólo el suscriptor posee.
<b>Activación de la clave privada</b>	La activación del dispositivo token/tarjeta criptográfica que contiene la clave privada del suscriptor se realiza a	La activación del archivo PKCS #12 que contiene la clave privada del suscriptor se realiza a través de una clave generada	La activación del uso de la clave privada generada en el HSM la realiza el suscriptor mediante la

	Política de Certificados de Miembro de Empresa			
	CÓDIGO	VERSIÓN	MES Y AÑO	Pág.
	JFE-SNS-2024-016-CF	05	Mayo de 2024	36 de 45

	través de un PIN generado aleatoriamente y comunicado al suscriptor por correo electrónico.	aleatoriamente y comunicada al suscriptor por correo electrónico.	introducción de sus propias credenciales.
<b>Desactivación de la clave privada</b>	El método para desactivar la clave privada del suscriptor es retirar el dispositivo token/tarjeta criptográfica del equipo, inmediatamente cualquier contenido asociado queda deshabilitado incluyendo la clave privada.	El método para desactivar la clave privada del suscriptor que ha importado su certificado a partir de un PKCS #12 es retirar el certificado del almacén de certificados que lo contenga, inmediatamente cualquier contenido asociado queda deshabilitado incluyendo la clave privada.	El método para desactivar la clave privada del suscriptor es mediante el cierre de sesión abierta con el SFC.
<b>Destrucción de clave <u>privada</u></b>	La destrucción de la clave privada 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 se produce mediante la eliminación del certificado asociado y mediante la eliminación de la propia clave.

### 6.2.1. Estándares para los módulos criptográficos

Las tarjetas criptográficas con certificados para firma electrónica, aptas como dispositivos seguros de creación de firma, cuentan con la certificación FIPS 140-2 del NIST Nivel 3 y/o Common Criteria EAL4+ (CWA14169).

### 6.2.2. Control multipersona de la clave privada

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

### 6.2.3. Custodia de la clave privada

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

### 6.2.4. Copia de seguridad de la clave privada

En ningún caso se podrá realizar copia alguna de seguridad de las claves privadas de firma electrónica de miembros de empresa.

### 6.2.5. Archivo de la clave privada

Las claves privadas de certificados de miembros de empresa en dispositivos criptográficos token/tarjeta criptográfica, de ningún modo serán archivadas para garantizar el no repudio.

	<b>Política de Certificados de Miembro de Empresa</b>			
	CÓDIGO	VERSIÓN	MES Y AÑO	Pág.
	JFE-SNS-2024-016-CF	05	Mayo de 2024	37 de 45

Las claves privadas de certificados de miembro de empresa en archivo PKCS #12 no serán almacenadas y sólo el usuario suscriptor tendrá acceso a dichas claves.

Las claves privadas de firma de persona natural en HSM SFC serán almacenadas de forma segura en donde sólo el usuario suscriptor podrá tener acceso a dichas claves archivadas.

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

En ningún caso será permisible transferir las claves privadas de firma de miembro de empresa. La clave privada de los suscriptores generada desde el token/tarjeta criptográfica nunca sale del dispositivo.

#### **6.2.7. Almacenamiento de la clave privada en un módulo criptográfico**

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

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

La clave privada debe ser almacenada por el propio suscriptor mediante la conservación del dispositivo token/tarjeta criptográfica u otros métodos, debido a que puede ser necesaria para descifrar la información histórica cifrada con la clave pública.

#### **6.2.8. Método de activación de la clave privada**

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

#### **6.2.9. Método de desactivación de la clave privada**

El método para desactivar la clave privada del suscriptor es retirar el dispositivo token/tarjeta criptográfica del equipo, inmediatamente cualquier contenido asociado queda deshabilitado incluyendo la clave privada.

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

	<b>Política de Certificados de Miembro de Empresa</b>			
	CÓDIGO	VERSIÓN	MES Y AÑO	Pág.
	JFE-SNS-2024-016-CF	05	Mayo de 2024	38 de 45

### 6.2.10. Método de destrucción de la clave privada

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

### 6.2.11. Clasificación de los módulos criptográficos

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

## 6.3. Otros aspectos de la administración del par de claves

### 6.3.1. Archivo de la clave pública

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

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

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

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

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

### 6.3.3. Datos de activación

### 6.3.4. Generación de datos de activación e instalación

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

#### Dispositivo TOKEN

- En el momento de generación de claves e importación del certificado, el PIN por defecto del token/tarjeta criptográfica se cambian aleatoriamente y se le envían por email al suscriptor. El suscriptor podrá cambiar el PIN del dispositivo siempre que lo considere oportuno.

	<b>Política de Certificados de Miembro de Empresa</b>			
	CÓDIGO	VERSIÓN	MES Y AÑO	Pág.
	JFE-SNS-2024-016-CF	05	Mayo de 2024	39 de 45

- El PIN debe ser custodiado por el suscriptor de modo que no sea conocido por nadie más y se garantice el control exclusivo del token/tarjeta criptográfica.

#### **Archivo PKCS#12**

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

#### **HSM-SFC**

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

#### **6.3.5. Protección de datos de activación**

La protección de los datos de activación del dispositivo token/tarjeta criptográfica o del archivo PKCS#12 son de responsabilidad del suscriptor, para esto se considerará lo siguiente:

- La clave de activación del token/tarjeta criptográfica debe ser cambiada y no conocida por nadie excepto por el suscriptor. El suscriptor podrá cambiar la clave del token/tarjeta criptográfica.
- La clave del archivo PKCS#12 debe ser generada y no conocida por nadie excepto por el suscriptor.
- Las credenciales de activación del HSM SFC deben ser generadas y no conocidas por nadie excepto por el suscriptor.

#### **6.4. Controles de seguridad informática**

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

## **7. PERFILES DE CERTIFICADO, CRL Y OCSP**

	<b>Política de Certificados de Miembro de Empresa</b>			
	<b>CÓDIGO</b>	<b>VERSIÓN</b>	<b>MES Y AÑO</b>	<b>Pág.</b>
	JFE-SNS-2024-016-CF	05	Mayo de 2024	40 de 45

## 7.1. Contenido del certificado

El contenido de los certificados de miembro de empresa es el siguiente:

CERTIFICADOS DE MIEMBRO DE EMPRESA		
Campos de certificado X.509 v3 (tbsCertificate)		
Descripción	Componente	Valor
Versión del certificado	<b>version</b>	v3
Número que identifica unívocamente al certificado	<b>serialNumber</b>	Número entero aleatorio de 20 bytes
Firma	<b>signature</b>	
Algoritmo usado por el CJ para firmar el certificado	algorithm	sha256withRSAEncryption
Emisor	<b>Issuer</b>	
	commonName (CN)	ENTIDAD DE CERTIFICACION ICERT-EC <sup>1</sup>
	organizationalUnitName (OU)	SUBDIRECCIÓN NACIONAL DE SEGURIDAD DE LA INFORMACION DNTICS <sup>1</sup>
	organizationName (O)	CONSEJO DE LA JUDICATURA <sup>1</sup>
	localityName (L)	DM QUITO <sup>1</sup>
Validez	countryName (C)	EC
	<b>validity</b>	
	notBefore	Fecha y hora de emisión del certificado, codificado en UTCTime
Asunto	notAfter	Not Before + 2 años, codificado en UTC Time
	<b>subject</b>	
	commonName (CN)	Nombre y apellidos del miembro de empresa <sup>1</sup>
	serialNumber	Número de cédula o pasaporte del miembro de empresa <sup>1 3</sup>
	organizationName (O)	Razón social de la empresa <sup>1</sup>
	localityName (L)	Ciudad del departamento de la empresa <sup>1 2</sup>
Clave pública del titular del certificado	countryName (C)	EC
	<b>subjectPublicKeyInfo</b>	
	algorithm-algorithm	rsa Encryption
	subjectPublicKey	Clave pública RSA, con tamaño de 2048 bits

<sup>1</sup> Codificado en utf8String, con las letras en Español en mayúsculas, sin tilde ni diéresis en las vocales.

<sup>2</sup>

	Política de Certificados de Miembro de Empresa			
	CÓDIGO	VERSIÓN	MES Y AÑO	Pág.
	JFE-SNS-2024-016-CF	05	Mayo de 2024	41 de 45

Sustituir por el mismo dato de la empresa, si no se quieren incluir datos del departamento en los certificados.

<sup>3</sup> Alfanumérico mayúsculas en inglés

## 7.2. Número de versión

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

### Extensiones del certificado

Las extensiones incluidas en los certificados digitales de miembro de empresa son las siguientes:

<i>keyUsage</i>	crítica
<i>basicConstraints</i>	no crítica
<i>certificatePolicies</i>	no crítica
<i>subjectAltName</i>	no crítica

Extensiones de certificado X.509 v3 (extensions)	
<b>authorityKeyIdentifier</b>	
keyIdentifier	Valor en extensión subjectKeyIdentifier del certificado de CA Subordinada CJ
<b>subjectKeyIdentifier</b>	Hash SHA-1 de la clave pública RSA en subjectPublicKey
<b>keyUsage (critical)</b>	digitalSignature nonRepudiation
<b>certificatePolicies</b>	
policyIdentifier	1.3.6.1.4.1.43745.1.2.1.4.x.y <sup>5</sup>
policyQualifiers	
policyQualifierId	id-qt-cps
qualifier-cPSuri	<a href="http://www.icert.fje.gob.ec/dpc/declaracion_practicas_certificacion.pdf">http://www.icert.fje.gob.ec/dpc/declaracion_practicas_certificacion.pdf</a>
<b>subjectAltName</b>	
rfc822Name	E-mail del miembro de empresa
directoryName	
1.3.6.1.4.1.43745.1.3.1	Número de cédula o pasaporte del miembro de empresa <sup>1 6</sup>
1.3.6.1.4.1.43745.1.3.2	Nombre(s) del miembro de empresa <sup>1</sup>
1.3.6.1.4.1.43745.1.3.3	Primer apellido del miembro de empresa <sup>1</sup>
1.3.6.1.4.1.43745.1.3.4	Segundo apellido del miembro de empresa (opcional) <sup>1</sup>

<sup>1</sup> Codificado en utf8String, con las letras en español en mayúsculas, sin tilde ni diéresis en las vocales.

	Política de Certificados de Miembro de Empresa			
	CÓDIGO	VERSIÓN	MES Y AÑO	Pág.
	JFE-SNS-2024-016-CF	05	Mayo de 2024	42 de 45

1.3.6.1.4.1.43745.1.3.5	Cargo del miembro de empresa <sup>1</sup>
1.3.6.1.4.1.43745.1.3.7	Dirección del departamento de la empresa <sup>113</sup>
1.3.6.1.4.1.43745.1.3.8	Teléfono del departamento de la empresa <sup>123</sup>
1.3.6.1.4.1.43745.1.3.9	Ciudad del departamento de la empresa <sup>123</sup>
1.3.6.1.4.1.43745.1.3.10	Razón social de la empresa <sup>1</sup>
1.3.6.1.4.1.43745.1.3.11	RUC de la empresa <sup>12</sup>
1.3.6.1.4.1.43745.1.3.12	País: <i>ECUADOR</i> <sup>1</sup>
1.3.6.1.4.1.43745.1.3.50	Tipo de titular de certificado: <i>MIEMBRO DE EMPRESA</i> <sup>1</sup>
1.3.6.1.4.1.43745.1.3.51	Tipo de contenedor criptográfico (uno de los valores): <i>HARDWARE-TOKEN/TARJETA; HARDWARE-HSM SFC; SOFTWARE-ARCHIVO (PKCS#12)</i> <sup>1</sup>
1.3.6.1.4.1.43745.1.3.52	RUP de la empresa (opcional) <sup>12</sup>
1.3.6.1.4.1.43745.1.3.54	Nombre del departamento de la empresa (opcional) <sup>23</sup>
<b>basicConstraints</b>	
<b>extKeyUsage</b>	id-kp-clientAuth id-kp-emailProtection
<b>cRLDistributionPoints</b>	
distributionPoint-fullName	
uniformResourceIdentifier	<a href="http://www.icert.fje.gob.ec/crl/icert.crl">http://www.icert.fje.gob.ec/crl/icert.crl</a>
<b>authorityInfoAccess</b>	
accessMethod	id-ad-ocsp
accessLocation -uniformResourceIdentifier	<a href="http://ocsp.icert.fje.gob.ec">http://ocsp.icert.fje.gob.ec</a>

## 7.2.1 Identificadores de objeto de los algoritmos

Los certificados digitales de miembro de empresa utilizan los siguientes algoritmos:

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

## 7.2.2 Formatos de nombre

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

<sup>1</sup> Solo caracteres numéricos.

<sup>3</sup> Sustituir por los datos de departamento o de empresa de ser el caso cuando no posea datos de departamento.

<sup>4</sup> Incluir los datos de departamento si existe, caso contrario el campo no aparece en el certificado.

<sup>5</sup> Dependiendo del tipo de contenedor criptográfico: *HARDWARE-TOKEN/TARJETA* x=1 y=1; *HARDWARE-HSM SFC* x=1 y=2; *SOFTWARE-ARCHIVO (PKCS#12)* x=2 y=1.

<sup>6</sup> Alfanumérico mayúsculas en inglés.

	<b>Política de Certificados de Miembro de Empresa</b>			
	CÓDIGO	VERSIÓN	MES Y AÑO	Pág.
	JFE-SNS-2024-016-CF	05	Mayo de 2024	43 de 45

### 7.2.3 Restricciones de nombre

Los nombres contenidos en los certificados emitidos bajo esta política están restringidos a “*Distinguished Names*” X.500, que son únicos y no ambiguos.

### 7.2.4 Objeto identificador de la Política de Certificados

La presente Política de Certificados de Miembro de Empresa está signada mediante el número único 1.3.6.1.4.1.43745.1.2.1.4.

### 7.2.5 Sintaxis y semántica de los calificadores de la política

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

- **Policy identifier:** Contiene el identificador de la Política de Certificados de miembro de Empresa.
- **URL DPC:** contiene la URL donde se puede obtener la última versión de la DPC y PC asociada.

## 7.3 Perfil de la CRL

### 7.3.1 Número de versión

La Infraestructura de Clave Pública del Consejo de la Judicatura utiliza CRLs X.509 v2.

### 7.3.2 CRL y extensiones

De conformidad a lo prescrito en la sección 7.2.2 de la Declaración de Prácticas de Certificación del Consejo de la Judicatura.

### 7.3.3 Perfil OCSP

### 7.3.4 Numero de versión

El certificado OCSP de la ICERT-EC se emite de acuerdo con el estándar X.509 v3.

### 7.3.5 Extensiones OCSP

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

*keyUsage* crítica  
*basicConstraints* crítica

## 8. AUDITORIA DE CONFORMIDAD Y OTRAS VALORACIONES

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

	<b>Política de Certificados de Miembro de Empresa</b>			
	CÓDIGO	VERSIÓN	MES Y AÑO	Pág.
	JFE-SNS-2024-016-CF	05	Mayo de 2024	44 de 45

## 9. OTROS NEGOCIOS Y ASUNTOS LEGALES

### 9 Tarifas

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

#### 9.1 Responsabilidad financiera

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

#### 9.2 Confidencialidad de la información

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

#### 9.3 Protección de la información personal

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

#### 9.4 Derechos de propiedad intelectual

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

#### 9.5 Obligaciones y garantías

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

#### 9.6 Limitaciones de responsabilidad

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

#### 9.7 Indemnizaciones

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

#### 9.8 Duración y terminación

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

#### 9.9 Procedimiento de cambio en las especificaciones

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

#### 9.10 Prevención de disputas

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

#### 9.11 Ley aplicable

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

	<b>Política de Certificados de Miembro de Empresa</b>			
	<b>CÓDIGO</b>	<b>VERSIÓN</b>	<b>MES Y AÑO</b>	<b>Pág.</b>
	JFE-SNS-2024-016-CF	05	Mayo de 2024	45 de 45

## 9.12 Estipulaciones diversas

### 9.12.1 Cláusula de aceptación completa

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

### 9.12.2 Independencia

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

### Firmas de Responsabilidad:

	Nombre	Cargo	Firma
<b>Elaborado por:</b>	Cristian Santiago Freire Rodríguez	Supervisor de Seguridad de la Información	
<b>Revisado por:</b>	Manuel Alejandro Pineda Serrano	Jefe Departamental de Seguridad de la Información	
<b>Aprobado por:</b>	Peter Antonio Cabrera Zambrano	Subdirector Nacional de Seguridad de la Información	