ACUERDO NÚMERO SAR-465-2024
Tegucigalpa, M. D.C., 06 de septiembre de 2023

EL DIRECTOR EJECUTIVO DEL SERVICIO DE ADMINISTRACIÓN DE RENTAS (SAR)

CONSIDERANDO: Que el Artículo 195 del Decreto Legislativo número 170-2016 de fecha 15 de diciembre del 2016, publicada en el Diario Oficial "La Gaceta" No. 34,224, de fecha 28 de diciembre del 2016 que contiene el Código Tributario, crea la Administración Tributaria como una entidad Desconcentrada adscrita a la Presidencia de la República, con autonomía funcional, técnica, administrativa y de seguridad nacional, con personalidad jurídica propia, responsable del control, verificación, fiscalización y recaudación de los tributos, con autoridad y competencia a nivel nacional denominándose **SERVICIO DE ADMINISTRACION DE RENTAS (SAR),** mediante el Acuerdo Ejecutivo No. 01-2017.

CONSIDERANDO: Que de conformidad al numeral 1) del artículo 197 del Código Tributario define que la Administración Tributaria estará a cargo de un(a) Director(a) Ejecutivo(a), con rango ministerial, nombrado por el (la) Presidente(a) de la República, quien será responsable de definir y ejecutar las políticas, estrategias, planes, programas y proyectos administrativos y metas, conforme a las políticas económicas, fiscales y tributarias del Estado.

CONSIDERANDO: Que el Artículo 198 de la supra citada norma establece entre otras atribuciones del Servicio de Administración de Rentas (SAR), 1) ..., 3) Crear planes y programas de gestión administrativa acorde con los lineamientos de la política económica y metas de recaudación anuales acordadas; ..., 12) Aprobar Acuerdos para la aplicación eficiente de las disposiciones en materia tributaria, de conformidad con el presente Código...; 15) Cualquier otra facultad o atribución que establezca la Ley, en sus competencias.

CONSIDERANDO: Que en el Artículo 199 del Decreto en mención, se establecen las atribuciones del Director Ejecutivo del **SERVICIO DE ADMINISTRACIÓN DE RENTAS (SAR):** 1) Ejercer la representación legal, administración general, dirección y manejo de la institución..., 2) Aprobar las políticas institucionales.

CONSIDERANDO: Que mediante Acuerdo Ejecutivo No. 23-2024 de fecha 18 de enero del 2024 se nombró al suscrito, como Director Ejecutivo del Servicio de Administración de Rentas (SAR), con rango de Secretario de Estado.

CONSIDERANDO: Que mediante Acuerdo Ejecutivo No. 435-2022 de fecha 9 de septiembre del 2022, fue nombrada la ciudadana **NIDIA SARAHÍ BERRÍOS MARTINEZ**, en el cargo de **SECRETARIA GENERAL** del Servicio de Administración de Rentas.

CONSIDERANDO: Que los órganos administrativos desarrollarán sus actividades sujetándose a la jerarquía normativa establecida en el artículo 7 de la Ley General de la Administración Pública y con arreglo a las normas de la economía, celeridad y eficacia, a fin de lograr una pronta y efectiva satisfacción del interés general.

CONSIDERANDO: Que es necesaria la creación de una Política de Certificación de Firma Electrónica Avanzada de Persona Jurídica del Servicio de Administración de Rentas (SAR), estableciendo el funcionamiento y operaciones de la Infraestructura de Clave Pública la administración Tributaria (PKI-SAR) como prestador de Servicio de Certificación, dirigido a Persona Jurídica, así como buscar regular los procedimientos vinculados a los demás roles y funciones establecidos en la presente política.

CONSIDERANDO: Que la Ley General de la Administración Pública en su artículo 116 determina que, los actos de los órganos de la Administración Pública adoptarán la forma de Decretos, Acuerdos, Resoluciones y Providencias.

POR TANTO: En el uso de las facultades que la Ley le confiere y en aplicación a lo establecido en los Artículos 109, 321 y 351 de la Constitución de la República; 195, 197, 198 y 199 del Código Tributario; 7, 116, 118 y 122 de la Ley General de Administración Pública; 19 de la Ley de Procedimiento Administrativo; Acuerdo Ejecutivo 01-2017; Acuerdo Ejecutivo No. 23-2024; Acuerdo Ejecutivo No. 435-2022 y demás disposiciones legales aplicables.

ACUERDA

PRIMERO: Aprobar la Política de Certificado de Firma Electrónica Avanzada de Persona Jurídica en el Servicio de Administrador de Rentas (SAR). Versión POL-GIF-GGI-NDP-025-V1.

SEGUNDO: Socializar a todos los empleados de la Institución por los medios más expeditos, la Política de Certificado de Firma Electrónica Avanzada de Persona Jurídica.

TERCERO: El presente Acuerdo entrará en vigencia a partir de su fecha. **CÚMPLASE.**

CHRISTIAN DAVID DUARTE CHÁVEZ
DIRECTOR EJECUTIVO

NIDIA SARAHI BERRIOS MARTÍNEZ
SECRETARIA GENERAL

POLÍTICA

DE CERTIFICADO DE FIRMA ELECTRÓNICA AVANZADA DE PERSONA JURÍDICA

POL-GIF-GGI-NDP-025-V1

SAR

SERVICIO DE ADMINISTRACIÓN DE RENTAS

DIRECCIÓN EJECUTIVA

SECRETARÍA GENERAL

Septiembre 2024

FECHA VIGENCIA: SEPTIEMBRE 2024	CÓDIGO: POL-GIF-GGI-NDP-025-V1	VERSIÓN 1.0	N° PÁGINAS 79

POLÍTICA DE CERTIFICACIÓN DE CERTIFICADO DE FIRMA ELECTRÓNICA AVANZADA DE PERSONA JURÍDICA

RUBRO	CARGO	FIRMA
APROBADO POR:	**Lic. Christian David Duarte Chávez** Director Ejecutivo	
REVISADO POR:	**Abg. Nidia Sarahí Berrios Martínez** Secretaria General	
	Ing. Diana Orestila Cárcamo Rodriguez Directora Nacional de Tecnología	
	Lic. Alessandra Vanesa Díaz Tovar Directora Nacional de Gestión Estratégica	
	Abg. Elmer Javier Umanzor López Director Nacional Jurídica	
	Abg. Celvin Antonio Ruíz Lobo Inspector General	

	Ing. Tania Poleth Bustillo Enamorado Jefa del Departamento de Gestión de Procesos	
	Abg. Fátima Isabel Estrada Saravia Experta en el Departamento de Asesoría Legal	
ELABORADO POR:	**Abg. Carlos Antonio García García** Especialista de Secretaría General	
	Ing. Osman René Moreno Ramos Experto Dirección Nacional De Tecnología	
	Lic. Antonio Bustillo Banegas Analista de Procesos	

Nota:

El responsable de aprobar es sujeto de cambio siempre que exista una delegación formal de tal atribución emitida por la máxima autoridad. Los responsables de revisar serán siempre las jefaturas y direcciones responsables del proceso según el catálogo vigente a la fecha. Pueden constar como revisores jefaturas y direcciones vinculadas con el proceso.

TABLA DE CONTENIDO

1. INTRODUCCIÓN

El presente documento corresponde a la Política de Certificado de Firma Electrónica Avanzada de Persona Jurídica que estipula el funcionamiento y operaciones de la Infraestructura de Clave Pública (en adelante PKI) del Servicio de Administración de Rentas (en adelante SAR) de la República de Honduras, en concordancia con las recomendaciones de la Request for Comments RFC 3647 "Internet X.509 Public Key Infrastructure: Certificate Policy and Certification Practices Framework", de IETF.

Todos los certificados que emite la PKI-SAR son conformes con la versión 3 del estándar X.509, permitiendo la inclusión de extensiones para certificación de atributos.

El presente documento es de carácter público y se encuentra dirigido a todas las personas jurídicas, así como a los terceros que confían en los certificados y servicios de Sellado Tiempo brindados por el SAR.

1.1 VISIÓN GENERAL

1.1.1 CONTROL DE DOCUMENTOS

Versión	Motivo	Fecha de vigencia	Documentos que elimina
1.0	Creación	Septiembre – 2024	N/A

1.1.2 OBJETIVO ESTRATÉGICO VINCULADO AL DOCUMENTO

OBJETIVO ESTRATÉGICO
Objetivo estratégico 1: Asistir, orientar y simplificar el cumplimiento voluntario de las obligaciones tributarias con servicios humanos, accesibles y efectivos.

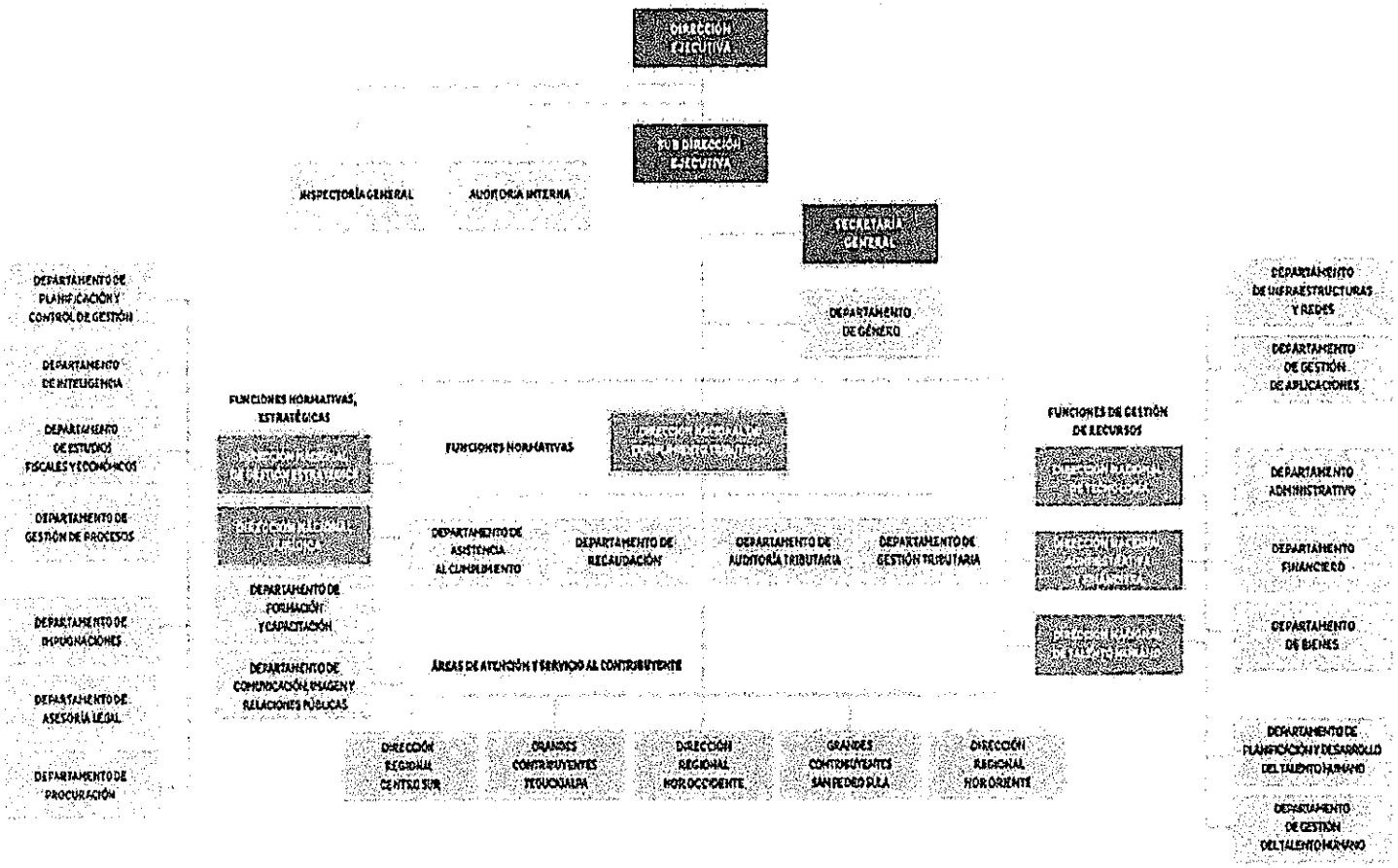
1.1.3 EJES TRANSVERSALES VINCULADO AL DOCUMENTO

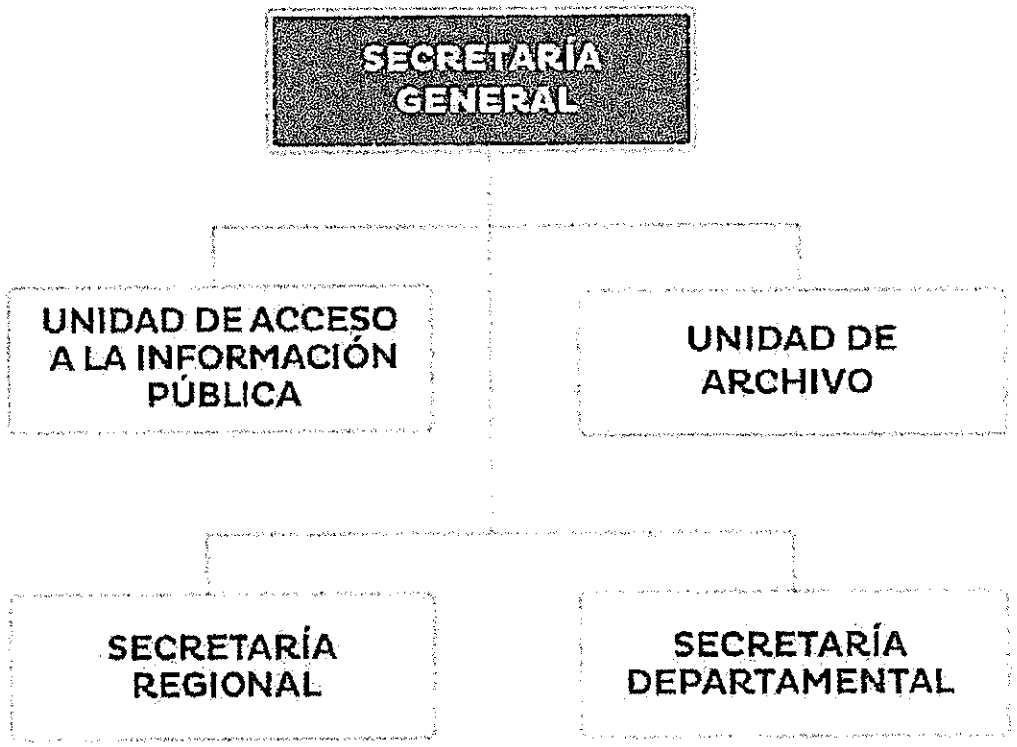
EJES TRANSVERSALES
Eje Transversal 2: **Entorno de Trabajo Saludable**
Eje Transversal 3: **Interculturalidad e Igualdad de Clases**

1.1.4 DOCUMENTO RELACIONADO

Nombre del Documento Relacionado	Código o número de acuerdo o del Documento Relacionado
Estatuto Orgánico	Acuerdo Número SAR-147-2024
Declaración de Prácticas de Certificación de Infraestructura de Clave Pública del Servicio de Administración de Rentas de la Republica De Honduras	Acuerdo Número SAR-057-2023

1.1.5 ESTRUCTURA ORGANIZACIONAL




SECRETARÍA GENERAL
UNIDAD DE ACCESO A LA INFORMACIÓN PÚBLICA
UNIDAD DE ARCHIVO
SECRETARÍA REGIONAL
SECRETARÍA DEPARTAMENTAL

1.1.6 IDENTIFICACIÓN DEL PROCESO

MACROPROCESO	4.Gestión de la Información
PROCESO A PRIMER NIVEL:	4.1. Gestión del Gobierno de la Información
PROCESO A SEGUNDO NIVEL:	N/A
RESPONSABLE DEL PROCESO:	Secretaría General

1.1.7 OBJETIVO

Establecer el funcionamiento y operaciones de la Infraestructura de Clave Pública de Servicio de Administración de Rentas (PKI-SAR) como Prestador de Servicio de Certificación, dirigido a Personas Jurídicas. Asimismo, se busca regular los procedimientos vinculados a los demás roles y funciones establecidos en la presente política.

1.1.8 ALCANCE

Esta política consiste en detallar que todos los Certificados de Firma Electrónica de Persona Jurídica emitidos por la entidad responsable, sean aceptados para cumplir con los requisitos del estándar RFC 3647 versión 3, la cual inicia desde el cumplimiento de los procedimientos para la emisión y gestión de certificados de firma electrónica, hasta garantizar que los certificados de firma electrónica emitidos por la PKI SAR sean reconocidos y aceptados de acuerdo con los estándares internacionales, jurídicos y técnicos a nivel nacional que permitan la inclusión de información adicional acerca de la persona que lo utiliza.

1.1.9 NORMAS Y DISPOSICIONES

a. Lo establecido en este documento es de aplicación obligatoria para los Suscriptores(as) de certificado electrónico emitidos por el Servicio de

Administración de Rentas, así como los terceros que confían en la emisión de los certificados emitidos por el PKI-SAR.

b. Los cambios y/o modificaciones que experimente el marco normativo nacional, prevalecen sobre las disposiciones contenidas en el presente documento hasta su actualización.

c. Los aspectos que no se encuentren normados de forma expresa en este documento deberán ser regulados por las disposiciones legales que apliquen.

d. Esta PC establece los requisitos particulares de los certificados para persona jurídica emitidos por Thomas Signe S.A.S, siguiendo el estándar RFC 3647 "Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework", y conforme a los estándares descritos en el numeral 1.1.10 referencia técnica.

1.1.10 EXCLUSIONES

Este documento ha sido diseñado basado en las recomendaciones de la RFC 3647, con la finalidad de hacer de fácil comprensión para el lector. Existen secciones que se determinan como "No estipulado"; las cuales no tienen inherencia en nuestro marco de cumplimiento.

1.1.11 MARCO NORMATIVO

Identificación de norma (Resolución o Acuerdo)	Fecha de vigencia	Referencia específica
Decreto No.149 -2013 y sus reformas	2013	Ley de Firma Electrónica
Acuerdo Ejecutivo No.41-2014	2014	Reglamento de Firma Electrónica
Acuerdo SAR 374-2018	2018	Creación de Comité de Firma Electrónica
Demás disposiciones legales aplicables		

1.1.12 REFERENCIA TÉCNICA

Documentos de Referencia	Fecha de vigencia
Recomendaciones del RFC 2560	1999
Recomendaciones del RFC 3161 – TSA	2001
Recomendaciones del RFC 3647 – PC	2003
Versión 2 del estándar X.509	2008
Recomendaciones del RFC 5280 – CRL	2008
Recomendaciones del RFC 6960 - OSCP	2013
ISO/IEC 27001 – Sistema de gestión de seguridad	2018
Política Declaración de Prácticas de Certificación de la Infraestructura de Llave Pública del Servicio de Administración de Rentas	2023

1.2 NOMBRE DEL DOCUMENTO E IDENTIFICACIÓN DE LA PC

El nombre de este documento es "Política de Certificación de Certificado de Firma Electrónica Avanzada de Persona Jurídica", **versión 1** y entra en vigente a partir de su fecha de aprobación y debe de ser sustituida al momento de la elaboración y aprobación de una nueva versión.

El URL para acceder públicamente a este documento se encuentra en la dirección electrónica https://www.sar.gob.hn/firmaelectronica/

El Indicador de Objeto (OID) correspondiente a este documento es el siguiente: 1.3.6.1.4.1.52089.2.3

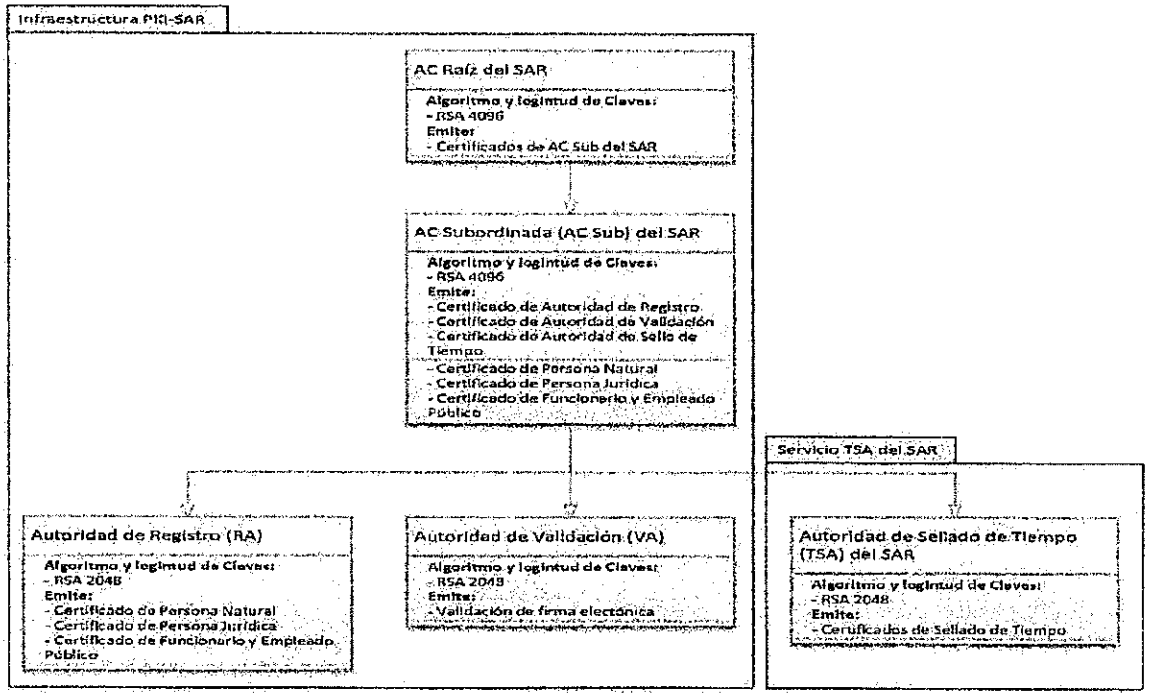
1.3 PARTICIPANTES DE LA PKI-SAR

Las entidades y personas intervinientes en la PKI-SAR son las que se enumeran a continuación:

- Autoridad de Certificación (AC).
- Autoridad de Registro (AR).
- Autoridad de Validación (AV).
- Autoridad de Sellado de Tiempo (AST).
- Comité de Firma Electrónica.

- Solicitantes y Suscriptores(as) de certificados.
- Terceros que confían en los certificados de la PKI del Servicio de Administración de Rentas.
- Autoridad Administrativa Competente (AAC).
- Prestador de Servicios de Certificación (PSC).

Para tener una mejor visión de la jerarquía de confianza de la PKI-SAR, se detalla a continuación la siguiente infraestructura:



1.3.1 AUTORIDAD DE CERTIFICACIÓN (AC)

De acuerdo a lo señalado en el artículo 23 del Reglamento de la Ley Sobre Firmas Electrónicas, pueden actuar como Autoridad Certificación, las Personas Naturales, y las Personas Jurídicas, tanto públicas como privadas, que sean autorizadas por la Autoridad Administrativa Competente (AAC), para operar como tales y que cumplan con los requerimientos establecidos en la Ley, sobre Firmas Electrónicas y su Reglamento, la Infraestructura Oficial de la Firma Electrónica y por la misma Autoridad Administrativa Competente (AAC).

También son los encargados de gestionar las solicitudes de revocación, renovaciones de los certificados electrónicos, así mismo como la generación de claves públicas y privadas de acuerdo con lo establecido en las prácticas y Políticas de Persona Natural y lo descrito en la presente Política para Persona Jurídica.

1.3.2 AUTORIDAD CERTIFICADORA RAÍZ DEL SAR

La PKI-SAR es la designada para realizar la emisión de los certificados, los cuales son objeto de la presente PC, regidos bajo el Certificado Raíz. Este consiste en un certificado auto firmado con el cual se inicia la cadena de confianza la cual debe de permanecer fuera de línea una vez se realice la ceremonia de llaves y se genere los certificados subordinados necesarios. Su encendido como apagado obedece a un procedimiento realizado para esta actividad.

Los certificados que se encuentran en subordinación al Certificado Raíz son los certificados de jerarquía o también conocidos como clave secundaria, o Autoridad de Certificación Subordinada.

En la siguiente tabla se detallan los datos con más relevancia de la Autoridad Certificadora de Servicio de Administración de Rentas:

Contenido del certificado Autoridad Certificadora Raíz del SAR				
	Atributo	Valor	Obligatorio	Crítica
Version	-	3	Si	-
Serial Number	-	2B C0 4A F2 74 CA 86 9B 11 33 95 4E F8 27 92 0F CB E8 BD CF	Si	-
Signature	Algorithm	Sha512WithRSAEncryption	Si	-
Issuer	CN	AUTORIDAD CERTIFICADORA RAIZ DEL SAR	Si	-
	O	SERVICIO DE ADMINISTRACION DE RENTAS	Si	-
	C	HN	Si	-
Validity	Not After	2023-02-28 12:25:02	Si	-
	Not Before	2043-02-28 12:25:20	Si	-
Subject	CN	AUTORIDAD CERTIFICADORA RAIZ DEL SAR	Si	-
	O	SERVICIO DE ADMINISTRACIÓN DE RENTAS	Si	-
	C	HN	Si	-
Subject Public Key Info	Algorithm	RSA	Si	-

1.3.3 AUTORIDAD CERTIFICADORA SUBORDINADA DEL SAR

La PKI-SAR del Servicio de Administración de Rentas implementa una Autoridad Certificadora Subordinada del SAR. Dicha AC es la siguiente en jerarquía a la Autoridad Certificadora Raíz, por tanto, la Autoridad Certificadora Subordinada es la encargada de la emisión de todos los certificados para persona natural, persona jurídica y empleados(as) públicos(as).

En la siguiente tabla se detallan los datos con más relevancia de la autoridad certificadora del SAR:

Contenido del certificado Autoridad Subordinada del SAR				
Nombre	**Atributo**	**Valor**	**Obligatorio**	**Crítica**
Version	-	3	Si	-
Serial Numbre	-	25 BB 62 C0 77 28 C6 BE DA E0 8F 67 DC AB 4B 84 4C B4 02 DB	Si	-
Signature	Algorithm	Sha384WithRSAEncryption	Si	-
Issuer	CN	AUTORIDAD CERTIFICADORA RAIZ DEL SAR	Si	-
	O	SERVICIO DE ADMINISTRACIÓN DE RENTAS	Si	-
	C	HN	Si	-
Validity	Not After	2023-02-28 12:42:52	Si	-
	Not Before	2033-02-28 12:42:52	Si	-
Subject	CN	AUTORIDAD SUBORDINADA DEL SAR	Si	-
	O	SERVICIO DE ADMINISTRACIÓN DE RENTAS	Si	-
	C	HN	Si	-
Subject Public Key Info	Algorithm	RSA	Si	-

1.3.4 AUTORIDAD DE REGISTRO (AR)

La Autoridad de Registro (AR) es la responsable de la gestión de las solicitudes, identificación, registro y aprobación de los certificados emitidos por la PKI-SAR y

cualquier responsabilidad específica establecida en la DPC y las Políticas de Certificación. Asimismo, es la entidad encargada de:

- Tramitar las solicitudes de certificados.
- Identificar al solicitante y comprobar que cumple con los requisitos necesarios para la solicitud de los certificados.
- Validar la documentación de acreditación de la persona que consta como firmante del certificado.
- Gestionar la generación de claves y la emisión del certificado.
- Gestionar el sistema para que haga la entrega del certificado al Suscriptor(a).

1.3.5 AUTORIDAD DE VALIDACIÓN (AV)

La Autoridad de Validación (AV) debe determinar en línea, el estado actual de cualquier certificado emitido por el componente AC Subordinada, a través del protocolo OCSP, de acuerdo con el estándar RFC 6960. Las respuestas OCSP emitidas están firmadas con la clave privada correspondiente al certificado de firma de respuestas OCSP del componente AV.

El mecanismo antes mencionado es complementario al proceso de publicación de las Listas de Certificado Revocados (CRL) de acuerdo con el estándar RFC 5280.

1.3.6 AUTORIDAD DE SELLADO DE TIEMPO (AST)

La Autoridad de Sellado de Tiempo (AST) es la entidad responsable de probar que un conjunto de datos existió antes de un momento dado y que ninguno de estos datos ha sido modificado desde entonces. El Sellado de Tiempo provee un valor añadido a la utilización de firma electrónica ya que ésta por sí sola no proporciona ninguna información acerca del momento de creación de la firma, y en el caso de que el firmante la incluyese, ésta habría sido proporcionada por una de las partes. Sin embargo, lo recomendable es que la marca de tiempo sea proporcionada por una tercera parte de confianza, de acuerdo con el estándar RFC 3161.

1.3.7 SOLICITANTES Y SUSCRIPTORES(AS) DE CERTIFICADOS

Los Solicitantes de certificados son definidos por la DPC de la PKI-SAR. Dentro del contexto de esta PC, el Suscriptor(a) del "Certificado de Firma Electrónica Avanzada de Persona Jurídica" es cualquier Persona Jurídica que posea un Registro Tributario Nacional vigente.

El Solicitante es cualquier persona natural que ostente y acredite la representación del suscriptor (persona jurídica) que posea un Documento Nacional de Identificación de Honduras o una persona extranjera residente en Honduras que presente su Carnet de Residencia, un extranjero no residente con su Pasaporte vigente.

1.3.8 TERCEROS QUE CONFÍAN EN LOS CERTIFICADOS EMITIDOS POR LA PKI-SAR

Los terceros que confían son comprendidos por las entidades o personas que confían en los certificados emitidos por la AC de la PKI-SAR con la finalidad de asegurar la identidad de un Suscriptor(a) como persona natural, persona jurídica y empleado(a) público(a).

1.3.9 AUTORIDAD ADMINISTRATIVA COMPETENTE (AAC)

La Dirección General de Propiedad Intelectual de Honduras (DIGEPIH) es la Autoridad Administrativa Competente (AAC) y legalmente facultada para actuar como Autoridad Acreditadora, es decir, para conceder autorización a las Autoridades Certificadoras a operar en el territorio nacional. Asimismo, está facultada para emitir la reglamentación correspondiente; diseñar y desarrollar la Infraestructura Oficial de la Firma Electrónica; organizar la función de inspección, control y vigilancia de las actividades realizadas por las Autoridades Certificadoras o Prestadores de Servicios de Certificación (PSC) e imponer las sanciones que correspondan de conformidad con la Ley Sobre Firmas Electrónicas y su Reglamento.

1.3.10 PRESTADOR DE SERVICIOS DE CERTIFICACIÓN (PSC)

La Autoridad Certificadora o Prestador de Servicios de Certificación (PSC), autorizados por la Autoridad Administrativa Competente (AAC), pueden realizar, entre otras, las siguientes actividades,

- Emitir certificados en relación con las firmas electrónicas certificadas de persona jurídica, persona natural.
- Emitir certificados sobre la verificación respecto de la alteración entre el envío y recepción del mensaje de datos.
- Ofrecer o facilitar los servicios de creación de Firmas Electrónicas Avanzada.

- Ofrecer o facilitar los servicios de registro y estampado cronológico en la generación, transmisión y recepción de mensajes de datos.
- Ofrecer los servicios de archivo y conservación de mensajes de datos.

Pueden actuar como Autoridad Certificadora o Prestador de Servicios de Certificación (PSC), las personas naturales y las personas jurídicas, tanto públicas como privadas. Estas personas naturales o jurídicas deben ser autorizadas por la Autoridad Administrativa Competente (AAC), para operar como tales y, además, cumplir con los requerimientos establecidos en la Ley Sobre Firmas Electrónicas y su Reglamento, la Infraestructura Oficial de la Firma Electrónica y por la misma Autoridad Administrativa Competente (AAC); todo lo anterior conforme las condiciones siguientes:

- Contar con la capacidad económica y financiera suficiente para prestar los servicios autorizados como autoridad certificadora, así como con el Talento Humano y la deontología jurídica, que demanda su condición de tal.
- Contar con la capacidad y elementos técnicos (equipos y programas informáticos) necesarios para la generación de Firmas Electrónicas, garantizando la autenticidad de estas, para la emisión y trámite de certificados; y la conservación de mensajes de datos y consulta de los registros en los términos establecidos en la Ley Sobre Firmas Electrónicas y su Reglamento.
- Disponibilidad de información para los firmantes nombrados en el certificado y para las partes que confíen en éste.

Para verificar que las Autoridades Certificadoras o Prestadores de Servicios de Certificación (PSC) cumplan con los requerimientos antes establecidos y determinar el grado de fiabilidad de dichos prestadores se toman los factores de acuerdo a lo señalado en el artículo 23 del Reglamento de la Ley Sobre Firmas Electrónicas siguientes:

- Recursos y capacidad financiera para asumir la responsabilidad por el riesgo de pérdida.
- Garantías y representaciones.
- Seguros.
- Descripción detallada de las políticas, procedimientos y mecanismos que el Prestador de Servicios de Certificación se obliga a cumplir.

- Disponer de personal suficiente de reconocida honorabilidad, el cual debe ser competente para las funciones que realiza, quienes están encargados de la emisión de opiniones técnicas que se requieran, la formulación de políticas y su implementación.
- Experiencia en tecnologías de clave pública y familiaridad con procedimientos de seguridad apropiados.
- Contar con el equipo y los programas informáticos necesarios.
- Mantenimiento de un registro de auditoría y realización de auditorías por una Autoridad independiente.
- Existencia de un plan para casos de emergencia (por ejemplo, "programas de recuperación en casos de desastre" o depósitos de claves).
- Disposiciones para proteger su propia clave privada.
- Seguridad interna.
- Disposiciones para suspender las operaciones, incluida la notificación a los usuarios.
- Declaración de limitación de la responsabilidad.
- Contar con procedimientos de revocación (en caso de que la clave criptográfica se haya perdido o haya quedado en entredicho).

1.4 USO DE LOS CERTIFICADOS

1.4.1 USO ADECUADO DE LOS CERTIFICADOS

El uso adecuado de los certificados descritos en esta PC es para la firma realizada por el titular, quien es siempre una Persona Natural facultada, la representación de la Persona Jurídica.

1.4.2 PROHIBICIONES DE USO DE LOS CERTIFICADOS

Los Certificados de Persona Jurídica no debe de emplearse para ningún propósito que no esté especificado en el numeral 1.4.1 denominado Uso Adecuado de los Certificados.

1.5 ADMINISTRACIÓN DE LAS POLÍTICAS

1.5.1 ORGANIZACIÓN RESPONSABLE DE ADECUACIÓN DE LAS POLÍTICAS

Los términos y redacción de la presente Política de Certificación de Persona Jurídica son establecidos por el Servicio de Administración de Rentas a través del Comité de Firma Electrónica; esta entidad es la responsable también de realizar revisiones periódicas de este documento, de manera que se mantengan actualizadas.

1.5.2 PROCEDIMIENTO DE APROBACIÓN Y MODIFICACIÓN DE LA POLÍTICA DE CERTIFICACIÓN DE PERSONA JURÍDICA

El SAR, a través del Comité de Firma Electrónica, vela por el cumplimiento de la Política de Certificación de Persona Jurídica, así como el pertinente proceso de revisión y aprobación de estas.

1.5.3 RESPONSABLE POR MODIFICACIONES A LA PC

La responsabilidad de la aprobación y modificación a esta PC corresponde de manera exclusiva al Comité Institucional de Firma Electrónica, de acuerdo con las facultades otorgadas a dicho comité por parte de Servicio del Administración de Rentas.

Todas las modificaciones realizadas a la PC deben ser publicadas en el sitio web del Servicio de Administración de Rentas, en la dirección electrónica https://sar.gob.hn/firmaelectronica/. En caso de haber exista disconformidad de las modificaciones por parte de algún Suscriptor(a), este puede realizar una solicitud de revocación de su certificado electrónico.

La acción de solicitar revocación interesada y voluntaria por parte de los usuarios que presenten disconformidad no da derecho al Suscriptor(a) de recibir compensación por este motivo.

1.5.4 DATOS DE CONTACTO

Nombre de Entidad: Servicio de Administración de Rentas - SAR

Dirección Física: Tegucigalpa, M.D.C., Edificio Cuerpo Bajo "A", Bulevar Juan Pablo II, Centro Cívico Gubernamental José Cecilio del Valle.

Correo: pki@sar.gob.hn

Teléfono: (504) 2216-5800

Para informar problemas de seguridad relacionados con un certificado, tales como sospecha de compromiso clave, uso indebido o fraude, se le solicita enviar un Informe de incidencia sobre certificado a la cuenta de correo electrónico: incidentes.pki@sar.gob.hn

1.6 GLOSARIO DE TÉRMINOS Y SIGLAS

1.6.1 GLOSARIO DE TERMINOS

- **Autenticación:** Proceso de intento de verificar la identidad digital de los Solicitantes o Suscriptores(as) de un certificado de la República de Honduras, de este modo la PKI-SAR se asegura de que los Solicitantes o Suscriptores(as) son quien ellos dicen ser.
- **Autoridad:** Entidad dentro de la PKI con tareas específicas de acuerdo con su rol como certificador, validador o registro.
- **Certificado Electrónico:** Todo mensaje de datos proporcionado por un "Prestador de servicios de certificación" que le atribuye certeza y validez a la firma electrónica.
- **Clave Privada:** Componente confidencial del Suscriptor(a), utilizado para el proceso de cifrado o firmado electrónico.
- **Clave Pública:** Componente de carácter público que corresponde a una clave privada, utilizado para el descifrado de información o verificación de identidad de firmas electrónicas.

• **Control Multipersona (K De N) de la Clave Privada:**	Se utiliza para el acceso a la clave privada de la CA Raíz y CA subordinada la cual esta almacenada en el módulo criptográfico (HSM), para acceder a la misma se requiere de la presencia de un mínimo de dos (M) de un grupo de tres (N). Este control multipersona garantiza que nadie tiene un control individual de las actividades críticas de la CA Raiz y CA Subordinada.
• **Identificación:**	Implica la acción y efecto de identificar, que es reconocer a un solicitante o Suscriptor(a) de certificado en la República de Honduras.
• **FIPS 140-2:**	Es el estándar para validar la eficacia de hardware criptográfico.
• **Infraestructura de Clave Pública:**	Una infraestructura de claves públicas (PKI) es un sistema de recursos, políticas y servicios que da soporte al uso del cifrado de claves públicas para autenticar a las partes que participan en una transacción.
• **Interoperabilidad:**	Es la capacidad y procedimientos, de compartir datos y posibilitar el intercambio de información con terceros.
• **Oficina de Registro:**	Lugar designado por la PKI-SAR para la generación del certificado de persona jurídica, previa validación del proceso de generación de este.
• **Persona Jurídica:**	Entidad debidamente registrada en el territorio hondureño, con capacidad suficiente para contraer obligaciones y realizar actividades que generan plena responsabilidad jurídica, frente a sí mismos y frente a terceros.

- **Persona Natural:** Individuo debidamente identificado en el territorio de la República de Honduras, mediante su Documento Nacional de Identificación.
- **Prestador de Servicios de Certificación:** Un Prestador de Servicios de Certificación es una persona, física o jurídica, que expide certificados electrónicos o que presta otros servicios en relación con la firma electrónica.
- **Repositorio Criptográfico de Software PKCS12:** Archivo para el almacenamiento de muchos objetos criptográficos en un solo archivo.
- **Repositorios:** Archivo es un sitio centralizado donde se almacena y mantiene información digital de los CRL, Certificados, DPC y PC.
- **Revocación:** La revocación de un certificado se define por la acción mediante la cual se invalida un certificado antes de su fecha de caducidad.
- **Solicitante:** Individuo que solicita un certificado electrónico mediante los procesos provistos por la PKI-SAR.
- **Suscriptor(a):** Entidad final para quien se han emitido certificados.
- **Tercero que confía:** Individuo o entidad distinta del Suscriptor(a) que decide confiar en los certificados electrónicos emitidos por el PKI SAR.
- **Unicidad:** Calidad de único o el hecho de las propiedades de cierto objeto definido hace que éste sea único.

1.6.2 SIGLAS

- **AAC:** Autoridad Administrativa Competente.
- **AC:** Autoridad de Certificación.
- **AR:** Autoridad de Registro.
- **AV:** Autoridad de Validación.
- **C:** Country (País). Correspondiente a estándar x.500.
- **CDP:** CRL Distribution Point - Punto de Distribución de CRL.
- **CN:** Common Name - Nombre Común. Correspondiente a estándar x.500.
- **CRL:** Certificate Revocation List - Lista de Revocación de Certificados.
- **DN:** Distinguished Name - Nombre Distintivo. Correspondiente a estándar x.500.
- **DPC:** Declaración de Practicas de certificación.
- **FIPS:** Federal Information Processing Standard.
- **HSM:** Hardware Security Module. Componente informático de hardware que salvaguarda y gestiona Claves electrónicas.
- **IEC:** International Electrotechnical Commission.
- **L:** Localidad o Dirección. Correspondiente a estándar x.500.
- **O:** Organization - Organización. Correspondiente a estándar x.500.
- **OCSP:** Online Certificate Status Protocol. método para determinar el estado de vigencia de un certificado digital X.509.
- **OID:** Object Identifier - Identificador Único de Objeto.
- **OU:** Organizational Unit - Unidad Organizacional. Correspondiente a estándar x.500.

- **PC:** Política de Certificación.
- **PIN:** Personal Identificacion Number – Contraseña que protege el acceso a datos.
- **PKCS:** Public Key Cryptography Standards. Estandar Internacional.
- **PKI:** Public Key Infrastructure - Infraestructura de Clave Pública.
- **PSC:** Proveedor de Servicios de Certificación.
- **RFC:** Request For Comments. Estandar desarrollado por el Internet Engineering Task Force.
- **PKI SAR:** Infraestructura de Clave Pública del Servicio de Administración de Rentas.
- **SAR** Servicio de Administración de Rentas
- **ST:** State - Estado. Correspondiente a estándar x.500.

2. REPOSITORIOS Y PUBLICACIÓN DE INFORMACIÓN

2.1 REPOSITORIOS

El repositorio de PKI-SAR está compuesto de un servicio web de libre acceso, el cual no contiene información de naturaleza confidencial.

Servicio de validación en línea que implementa el protocolo OCSP	http://ocsp2.sar.gob.hn/CryptosecOpenKey/va_service
Certificado Autoridad Certificadora de SAR	https://sar.gob.hn/firmaelectronica/
Prácticas y Políticas de Certificación	https://sar.gob.hn/firmaelectronica/
ARL	http://pki.sar.gob.hn/crlsar/arl.crl
Certificado de CA Subordinada	https://sar.gob.hn/firmaelectronica/
CRL	http://pki.sar.gob.hn/crlsar/crl.crl

2.2 PUBLICACIÓN DE INFORMACIÓN DE CERTIFICACIÓN

La Política de Certificación de Certificado Firma Electrónica Avanzada de Persona Jurídica es de carácter público y se encuentran publicadas en el sitio web de PKI-SAR, al que se hace mención en el numeral 2.1. Repositorios.

Las listas de Revocación de Certificados (CRL) son de carácter público y se encuentran publicadas en el servidor web de PKI-SAR al que se hace mención en el numeral 2.1. Repositorios.

El estado de los certificados emitidos puede ser consultado haciendo uso del servicio de validación en línea correspondiente al protocolo OCSP o en su defecto haciendo uso de las CRL y se encuentran publicadas en el servidor web de PKI-SAR, al que se hace mención en el numeral 2.1. Repositorios.

2.3 TIEMPOS Y FRECUENCIA DE PUBLICACIÓN

La Política de Certificación de Persona Jurídica es publicada consecuentemente al momento de su aprobación. Dicha documentación será publicada en el sitio web al que se hace mención en el numeral 2.1. Repositorio y Publicación de Información.

La AC debe de agregar los certificados que hayan sido revocados a la CRL correspondiente, la ventana de tiempo debe ser acorde al punto 4.9.7. denominado Frecuencia de Emisión de CRL de la DPC de la PKI-SAR.

2.4 CONTROLES DE ACCESO A LOS REPOSITORIOS

Todos los repositorios anteriormente citados son de acceso libre para la consulta y, en su caso, descarga información. Así mismo, la PKI-SAR ha establecido controles para impedir que personas no autorizadas puedan añadir, modificar o borrar información incluida en sus repositorios y para proteger la autenticidad e integridad de dicha información.

3. IDENTIFICACIÓN Y AUTENTICACIÓN

3.1 NOMBRES

3.1.1 TIPOS DE NOMBRES

La totalidad de los Suscriptores(as) de certificados requieren de un Distinguished Name el cual debe cumplir con el estándar "Internet X.509 Publick Key Infraestructure Certificate and Certificate Revocation List (CRL)".

A continuación, se define el procedimiento de asignación de los nombres distintivos para los certificados de persona jurídica.

Campo	Valor	Descripción
C	HN	País
O	PERSONA JURIDICA	Organización
OU	FIRMA ELECTRÓNICA	Unidad Organizacional
CN	CN=[F] NOMBRE PERSONA JURIDICA<Nombre descriptivo de la persona jurídica, asegurando que dicho nombre tenga sentido y no dé lugar a ambigüedad>	Nombre Común
Description	REGISTRO TRIBUTARIO NACIONAL	RTN
BusinessCategory	<Denominación o razón social>	Denominación o razón social

3.1.2 NECESIDAD DE QUE LOS NOMBRES SEAN SIGNIFICATIVOS

Se recomienda que los nombres de los Suscriptores(as) de los certificados sean significativos para todos los casos. La descripción de los atributos asociados al Suscriptor(a) del certificado es legible por humanos.

3.1.3 REGLA PARA INTERPRETAR VARIOS FORMATOS DE NOMBRES

La PKI-SAR hace uso de la regla ISO/IEC 9595 (X.500) Distinguished Name (DN) con el fin de interpretar los nombres distintivos de los Suscriptores(as) de certificado.

3.1.4 UNICIDAD DE LOS NOMBRES

La agrupación del Nombre Distintivo (DN) más el contenido de la extensión Policy Indentifier debe ser único y no confuso. El uso del número de RTN en el Common Name (CN) garantiza la unicidad de este

3.1.5 RECONOCIMIENTO, AUTENTICACIÓN Y PAPEL DE LAS MARCAS REGISTRADAS

El SAR no asume compromiso alguno sobre el uso de signos distintivos, registrados o no en la emisión de los certificados expedidos. Solo se permite en la solicitud de certificados que incluyan signos distintivos cuyo derecho de uso sea propiedad del titular o se encuentre debidamente autorizado.

3.2 VALIDACIÓN INICIAL DE IDENTIDAD

3.2.1 MÉTODOS PARA COMPROBAR LA CLAVE PRIVADA

El SAR no genera ni almacena las claves privadas asociadas a los Certificados de Persona Jurídica expedidos bajo la presente PC; estas claves son generadas bajo el exclusivo control del firmante y, en su caso, con la intervención de la Oficina de Registro correspondiente, cuya custodia está bajo responsabilidad del titular del certificado.

Para la expedición de los Certificados de Persona Jurídica, se requiere que el solicitante facultado genere la clave privada en el sistema del PKI-SAR después de haber sido registrado en el mismo una vez validada dicha generación por parte de la Oficina de Registro, tras el proceso de acreditación de la identidad del citado solicitante y recabada su voluntad.

3.2.2 AUTENTICACIÓN DE LA IDENTIDAD DE LA ORGANIZACIÓN

La identidad de una persona jurídica se verifica a través del certificado extendido por el Registro Mercantil en el que estén inscritos los documentos de constitución y de apoderamiento. En caso de institución pública se verifica a través del decreto de creación.

3.2.3 AUTENTICACIÓN DE LA IDENTIDAD DE LA PERSONA FÍSICA SOLICITANTE

El PKI-SAR comprueba los datos relativos a la constitución, creación, personalidad jurídica, y a la extensión y vigencia de las facultades de representación del solicitante, mediante la presentación de copias fotostáticas autenticadas en que constan dichos documentos y certificados originales extendidos por el Registro Mercantil; y para el caso de las instituciones públicas, el decreto de creación publicado en el Diario Oficial la Gaceta.

El solicitante de certificado de persona jurídica debe proporcionar la siguiente información:

- Datos personales:
  - Documento Nacional de Identificación, Pasaporte Vigente o Carnet de Residencia del representante facultado.
  - Carta poder, escritura pública o documento legal que acredite su facultad para actuar en representación de la Persona Jurídica.
- Datos de la Persona Jurídica:
  - Denominación o razón social.
  - Escritura de constitución, o copia decreto de creación en caso de ser institución pública.
  - Número de RTN
  - Dirección de correo electrónico de la Persona Jurídica y correo electrónico de su representante.
  - Dirección física.

3.2.4 INFORMACIÓN NO VERIFICADA SOBRE EL SOLICITANTE

Toda la información incorporada al certificado electrónico es verificada por el personal asignado en la Oficina de Registro.

3.2.5 COMPROBACIÓN DE LAS FACULTADES DE REPRESENTACIÓN

Para comprobar las facultades de representación, el representante debe comparecer personalmente a la Oficina de Registro con su Documento Nacional de Identificación, Carnet de Residencia o Pasaporte Vigente y el documento que acredite su capacidad para actuar como representante de la persona jurídica.

3.2.6 CRITERIOS PARA INTEROPERABILIDAD

Este contenido se detalla en la DPC de la PKI-SAR, en el numeral 3.2.6 Criterios para Interoperabilidad, de tal forma remitirse a lo ahí establecido.

3.3 IDENTIFICACIÓN Y AUTENTICACIÓN PARA SOLICITUDES DE RENOVACIÓN DE CLAVES

La Política de Certificación de Persona Jurídica no contempla ningún proceso de regeneración de claves.

Las condiciones de autenticación de una petición de renovación se desarrollan en el apartado correspondiente al proceso de renovación de certificados de este documento.

3.4 IDENTIFICACIÓN Y AUTENTICACIÓN PARA SOLICITUDES DE REVOCACIÓN

Previo a la revocación efectiva de los certificados, la persona asignada en la oficina de Registro identifica de forma fehaciente a los Solicitantes de la revocación para vincularlos con los datos únicos del certificado a revocar.

Las condiciones de autenticación de una petición de revocación se desarrollan en el apartado correspondiente al proceso de revocación de certificados de este documento.

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

4.1 SOLICITUD DE CERTIFICADOS

4.1.1 ¿QUIEN PUEDE REALIZAR UNA SOLICITUD?

La solicitud del Certificado de Persona Jurídica es realizada por una persona natural, quien siempre actúa en calidad de representante de una persona jurídica, y debe presentar su Documento Nacional de Identificación, Carnet de Residencia o Pasaporte Vigente, como requisito indispensable junto con el documento que acredite su capacidad para actuar entre otros requisitos que se puedan establecer para registrar y resolver la solicitud.

4.1.2 PROCESO DE ENROLAMIENTO Y RESPONSABILIDADES DE LOS SOLICITANTES

El titular del certificado solicita una cita a través de los medios que disponga la Administración Tributaria, dicho titular es siempre una persona natural, en su condición de representante de una persona jurídica.

El día de la cita, el Solicitante se presenta a la oficina de registro seleccionado en dicha aplicación presentando los siguientes documentos:

- Datos personales:
    - Documento Nacional de Identificación, Pasaporte Vigente o Carnet de Residencia del representante facultado.
    - Carta poder, escritura pública o documento legal que acredite su facultad para actuar en representación de la Persona Jurídica.

- Datos del perfil:
    - Denominación o razón social.

- Escritura de constitución, o copia de decreto de creación en caso de ser institución pública.
- Número de RTN.
- Dirección de correo electrónico de la Persona Jurídica.
- Dirección física.

4.2 GESTIÓN DE LAS SOLICITUDES DE CERTIFICADOS

4.2.1 FUNCIONES DE IDENTIFICACIÓN Y AUTENTICACIÓN

Para los certificados de Persona Jurídica, el solicitante aporta los datos que se le requieran, acredita su documento nacional de identificación personal, y/o Carnet de Residencia, Pasaporte Vigente en su condición de Representante de la Persona Jurídica. El personal asignado a la Oficina de Registro constata la identidad del solicitante y conserva la documentación que la acredite.

4.2.2 RECHAZO O ACEPTACIÓN DE SOLICITUDES DE CERTIFICADO

En el caso de los certificados para personas jurídicas, una vez que se ha verificado la identidad del solicitante, se procede al registro del certificado, que incluye la introducción de la clave privada por parte de la persona que actúa en representación de la entidad. Finalmente, el sistema envía el certificado por correo electrónico al correo de la Persona Jurídica.

La PKI-SAR tiene la potestad de rechazar una solicitud de certificación en los siguientes casos:

- La documentación de identificación no es válida.
- El solicitante que no ostenta la representación para solicitar la emisión de certificado.
- Si la información concerniente a identificación y autenticación de toda la información requerida en cada PC no está completa.
- Los datos no son consistentes con el formato de solicitud de certificación.

4.2.3 PLAZO PARA LA GESTIÓN DE LAS SOLICITUDES

El PKI-SAR no se hará responsable por el retraso que puedan surgir entre la solicitud del certificado y la entrega de este. En cualquier caso, el plazo para la

tramitación de las solicitudes de certificados viene limitado por la disponibilidad de citas en las oficinas de registro a la que desee acudir el solicitante; y de igual manera, a la carga administrativa interna de la AC.

4.3 EMISIÓN DE CERTIFICADOS

4.3.1 ACCIONES DE LA AC DURANTE LA EMISIÓN DE CERTIFICADO

La acción de emitir un certificado implica la autorización definitiva de la solicitud de certificación por parte de la AC. Al momento de la emisión del certificado con base a la solicitud, se realizan las notificaciones que se describen el apartado 4.3.2. denominado Notificación al Solicitante de la Emisión por la AC del Certificado.

La vigencia de los certificados inicia al momento de emisión de estos. El período de validez o vigencia del certificado puede ser sujeto de una extinción anticipada, temporal o definitiva, esto en el caso de que se den las causas necesarias que motiven a la suspensión o revocación de este.

4.3.2 NOTIFICACIÓN AL SOLICITANTE DE LA EMISIÓN POR LA AC DEL CERTIFICADO

Una vez emitido el certificado de Persona Jurídica, la PKI-SAR informa por medio de correo electrónico sobre la disponibilidad del certificado para su descarga.

4.4 ACEPTACIÓN DEL CERTIFICADO

4.4.1 ACCIÓN QUE AFIRMA LA ACEPTACIÓN DEL CERTIFICADO

En el proceso de solicitud del certificado de Persona Jurídica, el solicitante acepta las condiciones de uso y expresa su voluntad de obtener el certificado como requisitos necesarios para la generación de este.

4.4.2 PUBLICACIÓN DEL CERTIFICADO POR PARTE DE LA AC

Este punto no es aplicable, la PKI-SAR una vez emitido el certificado no los publica en repositorios.

4.4.3 NOTIFICACIÓN DE LA EMISIÓN DEL CERTIFICADO POR LA AC A OTRAS ENTIDADES

No se realizan notificaciones de emisión a otras entidades AC, ya que no existe alguna relación o dependencia con ellas.

4.5 USO DEL PAR DE CLAVES Y CERTIFICADO

Los Certificados de Persona Jurídica son certificados de uso intransferible que acreditan la identidad de su titular (Persona Jurídica), los que se emiten para el exclusivo uso en el ámbito de sus funciones.

4.5.1 USO DE LA CLAVE PRIVADA Y DEL CERTIFICADO POR EL SUSCRIPTOR(A)

El titular sólo puede utilizar la clave privada y el certificado para los usos autorizados en la presente PC y de acuerdo con lo establecido en los campos 'Key Usage' y 'Extended Key Usage' del certificado. Del mismo modo, el titular solo puede utilizar el par de claves y el certificado tras aceptar las condiciones de uso, establecidas en la DPC y la presente PC,

Una vez haya sido revocado el certificado o haya expirado, lo que ocurra primero, el Suscriptor(a) no puede usar la clave privada.

4.5.2 USO DE LA CLAVE PÚBLICA Y DEL CERTIFICADO POR LO TERCEROS QUE CONFÍAN

Los terceros que confían sólo pueden depositar su confianza en los certificados para el uso exclusivo en el ámbito de sus funciones del titular como representante de persona jurídica de acuerdo con lo establecido en el campo 'Key Usage' y 'Extended Key Usage' del certificado.

Es responsabilidad de los terceros que confían el realizar las operaciones de clave pública siguiendo los procedimientos adecuados para confiar en el certificado, así como también realizar las verificaciones del estado de certificado utilizando los medios establecidos en la DPC y la presente PC.

De la misma forma están sujetos del cumplimiento de las condiciones de uso establecidas en los documentos antes mencionados.

4.6 RENOVACIÓN DE CERTIFICADOS SIN CAMBIO DE CLAVE

No es posible renovar certificado sin cambio de clave, para los certificados de persona jurídica. Por tanto, cualquier necesidad de renovación de certificado conlleva a la expedición de un nuevo certificado. Consecuentemente, el resto de los incisos siguientes referentes a la modificación de certificados (incisos 4.6.1, 4.6.2, 4.6.3, 4.8.4, 4.8.5 4.8.6, 4.8.7) se consideran como no estipulado en este documento.

4.6.1 CIRCUNSTANCIAS PARA LA RENOVACIÓN DE CERTIFICADOS SIN CAMBIO DE CLAVE

No estipulado.

4.6.2 TRAMITACIÓN DE LAS PETICIONES DE RENOVACIÓN DE CERTIFICADOS SIN CAMBIO DE CLAVES

No estipulado.

4.6.3 QUIÉN PUEDE SOLICITAR LA RENOVACIÓN DE LOS CERTIFICADOS SIN CAMBIO DE CLAVE

No estipulado.

4.6.4 NOTIFICACIÓN DE LA EMISIÓN DE UN NUEVO CERTIFICADO AL SUSCRIPTOR(A)

No estipulado.

4.6.5 FORMA DE ACEPTACIÓN DEL CERTIFICADO SIN CAMBIO DE CLAVE

No estipulado.

4.6.6 PUBLICACIÓN DEL CERTIFICADO SIN CAMBIO DE CLAVE

No estipulado.

4.6.7 NOTIFICACIÓN DE LA EMISIÓN DEL CERTIFICADO POR LA AC A OTRAS AUTORIDADES

No estipulado.

4.7 RENOVACIÓN DE CERTIFICADOS CON CAMBIO DE CLAVES

Bajo la presente PC, se determina que, para realizar la renovación con regeneración de claves de los Certificados de Persona Jurídica, se debe realizar siempre emitiendo nuevas claves, siguiendo el mismo proceso que el descrito para la emisión de un certificado nuevo; por ello, se debe remitir a dicho apartado.

4.7.1 CIRCUNSTANCIAS PARA LA RENOVACIÓN CON CAMBIO DE CLAVES DE UN CERTIFICADO

No estipulado.

4.7.2 QUIÉN PUEDE PEDIR LA RENOVACIÓN DE LOS CERTIFICADOS

Se sigue el mismo proceso que el descrito para emisión de un certificado nuevo.

4.7.3 GESTIÓN DE LAS PETICIONES DE RENOVACIÓN DE CERTIFICADOS CON CAMBIO DE CLAVES

Se sigue el mismo proceso que el descrito para emisión de un certificado nuevo.

4.7.4 NOTIFICACIÓN DE LA EMISIÓN DE UN NUEVO CERTIFICADO AL SUSCRIPTOR(A)

Se sigue el mismo proceso que el descrito para emisión de un certificado nuevo.

4.7.5 MÉTODO DE ACEPTACIÓN DEL CERTIFICADO CON CAMBIO DE CLAVES

Se sigue el mismo proceso que el descrito para emisión de un certificado nuevo.

4.7.6 PUBLICACIÓN DEL CERTIFICADO CON LAS NUEVAS CLAVES POR PARTE DE LA AC

Se sigue el mismo proceso que el descrito para emisión de un certificado nuevo.

4.7.7 NOTIFICACIÓN DE LA EMISIÓN DEL CERTIFICADO POR LA AC A OTRAS AUTORIDADES

Se sigue el mismo proceso que el descrito para emisión de un certificado nuevo.

4.8 MODIFICACIÓN DE CERTIFICADOS

No es posible realizar modificaciones a los certificados de persona jurídica expedidos. Por tanto, cualquier necesidad de modificación con lleva la expedición de un nuevo certificado. Consecuentemente el resto de los incisos referentes a la

modificación de certificados (incisos 4.8.1, 4.8.2, 4.8.3, 4.8.4, 4.8.5, 4.8.6, 4.8.7) se consideran como no estipulado en este documento.

4.8.1 CIRCUNSTANCIAS PARA LA MODIFICACIÓN DEL CERTIFICADO

No estipulado

4.8.2 ¿QUIÉN PUEDE SOLICITAR LA MODIFICACIÓN DE LOS CERTIFICADOS?

No estipulado

4.8.3 GESTIÓN DE LAS PETICIONES DE MODIFICACIÓN DE CERTIFICADOS

No estipulado.

4.8.4 NOTIFICACIÓN POR LA EMISIÓN DE UN CERTIFICADO MODIFICADO AL SUSCRIPTOR(A)

No estipulado.

4.8.5 MÉTODO DE ACEPTACIÓN DEL CERTIFICADO MODIFICADO

No estipulado.

4.8.6 PUBLICACIÓN DEL CERTIFICADO MODIFICADO POR LA AC

No estipulado.

4.8.7 NOTIFICACIÓN DE LA MODIFICACIÓN DEL CERTIFICADO POR LA AC A OTRAS ENTIDADES

No estipulado.

4.9 REVOCACIÓN Y SUSPENSIÓN DE CERTIFICADOS

4.9.1 CIRCUNSTANCIAS PARA LA REVOCACIÓN

La revocación de un certificado se define por la acción mediante la cual se invalida un certificado antes de su fecha de caducidad por parte de la AC de la PKI-SAR.

La revocación de un certificado va aunada a su publicación en la respectiva Lista de Certificados Revocados (CRL).

Sin exclusión o detrimento de lo dispuesto en la norma aplicable un certificado puede ser revocado por las siguientes circunstancias:

- A petición del Suscriptor(a) o un tercero en su nombre y representación debidamente facultado, justificando el motivo de la revocación.
- Por disolución de la Persona Jurídica.
- Compromiso de la clave privada del titular.
- El titular de un certificado deja de representar a la Persona Jurídica circunstancia que le facultaba para la posesión del certificado.
- Por la confirmación de que alguna información o hecho contenido en el certificado es falso.
- La clave privada de PKI-SAR o su sistema de seguridad ha sido comprometido de manera material que afecte la confiabilidad del certificado.
- Por el cese de actividades de PKI-SAR.
- Por orden judicial o de Autoridad Administrativa Competente;
- Cualquier otra causa lícita prevista en la declaración de prácticas de certificación.

La finalidad principal de la revocación es la terminación inmediata del período de validez del certificado, resultando en la no validez de este. La revocación no tendrá efectos retroactivos ni perjudica las obligaciones creadas o comunicadas mediante esta PC.

4.9.2 QUIÉN PUEDE SOLICITAR LA REVOCACIÓN

La revocación de un certificado de persona jurídica solamente puede ser solicitado por:

- La PKI-SAR.
- La persona natural facultada en su condición de representante de una persona jurídica
- Autoridad Judicial.

La AC de la PKI-SAR puede revocar de oficio los certificados de persona jurídica si tuviera conocimiento o sospecha del compromiso de la clave privada del titular o cualquier otro hecho recogido en la presente PC.

4.9.3 PROCEDIMIENTO DE SOLICITUD DE REVOCACIÓN

La revocación de Certificado de Persona Jurídica la puede solicitar la persona natural en su condición de representante de una persona jurídica. Para ello se debe presentar la documentación que acredite la solicitud de revocación o cualquier otro documento que sustente el cese definitivo del certificado electrónico.
Una vez que la PKI-SAR ha procedido a la revocación del certificado de persona jurídica, se publica en el directorio seguro la correspondiente Lista de Certificados Revocados, conteniendo el número de serie del Certificado Revocado, así como la fecha y hora. Una vez que un certificado ha sido revocado, su vigencia queda definitivamente extinguida, sin posibilidad de revertir su estado.

4.9.4 PERÍODO EN QUE DEBE PROCESAR LAS SOLICITUDES DE REVOCACIÓN

No existe período de gracia para este proceso, debido a que las revocaciones son ejecutadas de manera inmediata a la tramitación de las solicitudes que sean verificadas como válidas.

4.9.5 PLAZO EN EL QUE DEBE RESOLVER LA SOLICITUD DE REVOCACIÓN

La PKI-SAR procede a la revocación inmediata del certificado en el momento de verificar la identidad del solicitante o de la veracidad de la solicitud realizada mediante resolución judicial o administrativa. En cualquier caso, la revocación efectiva del certificado se realiza en menos de 24 horas desde la recepción de la solicitud de revocación en días laborables y nunca superior a 72 horas en días de semana o días festivos.

4.9.6 REQUISITOS DE VERIFICACIÓN DE LAS REVOCACIONES POR LOS TERCEROS QUE CONFÍAN

Este contenido se detalla en la DPC de la PKI-SAR, en el numeral 4.9.6 denominado Requisitos de Verificación de las Revocaciones por los Terceros que Confían, de tal forma remitirse a lo ahí establecido.

4.9.7 FRECUENCIA DE EMISIÓN DE CRL

Este contenido se detalla en la DPC de la PKI-SAR, en el numeral 4.9.7 denominado Frecuencia de Emisión de CRL, de tal forma remitirse a lo ahí establecido.

4.9.8 TIEMPO MÁXIMO ENTRE LA GENERACIÓN Y LA PUBLICACIÓN DE LAS CRL

Este contenido se detalla en la DPC de la PKI-SAR, en el numeral 4.9.8 denominado Tiempo Máximo Entre la Generación y la Publicación de las CRL, de tal forma remitirse a lo ahí establecido.

4.9.9 DISPONIBILIDAD DE UN SISTEMA EN LÍNEA DE VERIFICACIÓN DEL ESTADO DE LOS CERTIFICADOS

Este contenido se detalla en la DPC de la PKI-SAR, en el numeral 4.9.9 denominado Disponibilidad de un Sistema en Línea de Verificación del Estado de los Certificados, de tal forma remitirse a lo ahí establecido.

4.9.10 REQUISITOS DE COMPROBACIÓN EN LÍNEA DE REVOCACIÓN

Este contenido se detalla en la DPC de la PKI-SAR, en el numeral 4.9.10 denominado Requisitos de Comprobación en Línea de Revocación, de tal forma remitirse a lo ahí establecido.

4.9.11 OTRAS FORMAS DE DIVULGACIÓN DE INFORMACIÓN DE REVOCACIÓN DISPONIBLES

No estipulado.

4.9.12 CAUSAS PARA LA SUSPENSIÓN

Este contenido se detalla en la DPC de la PKI-SAR, en el numeral 4.9.12 denominado Causas para la Suspensión, de tal forma remitirse a lo ahí establecido.

4.9.13 QUIÉN PUEDE SOLICITAR LA SUSPENSIÓN

La solicitud de suspensión de un certificado de persona jurídica solamente puede ser solicitado por:

- La PKI-SAR.
- La persona natural facultada, en su condición de representante de una persona jurídica
- Autoridad Judicial.

4.9.14 PROCEDIMIENTO PARA LA SOLICITUD DE SUSPENSIÓN

Se realiza el mismo proceso de revocación establecido en la presente PC en el numeral 4.9.3. denominado Procedimiento de Solicitud de Revocación, de tal forma remitirse a lo ahí establecido.

4.9.15 LÍMITES DEL PERÍODO DE SUSPENSIÓN

Este contenido se detalla en la DPC de la PKI-SAR, en el numeral 4.9.15 denominado Limites del Periodo de Suspensión, de tal forma remitirse a lo ahí establecido.

4.10 SERVICIOS DE INFORMACIÓN DEL ESTADO DE CERTIFICADOS

4.10.1 CARACTERÍSTICAS OPERATIVAS

Este contenido se detalla en la DPC de la PKI-SAR, en el numeral 4.10.1 denominado Características Operativas, de tal forma remitirse a lo ahí establecido.

4.10.2 DISPONIBILIDAD DEL SERVICIO

Este contenido se detalla en la DPC de la PKI-SAR, en el numeral 4.10.2 denominado Disponibilidad del Servicio, de tal forma remitirse a lo ahí establecido.

4.10.3 CARACTERÍSTICAS ADICIONALES

Este contenido se detalla en la DPC de la PKI-SAR, numeral 4.10.3 denominado Características Adicionales.

4.11 FINALIZACIÓN DE LA VALIDEZ DE UN CERTIFICADO

Este contenido se detalla en la DPC de la PKI-SAR, en el numeral 4.11 denominado Finalización de la Validez de un Certificado, de tal forma remitirse a lo ahí establecido.

4.12 CUSTODIA Y RECUPERACIÓN DE CLAVES

4.12.1 PRÁCTICAS Y POLÍTICAS DE RECUPERACIÓN DE CLAVES

La PKI-SAR no recupera las claves privadas asociadas a los certificados de persona jurídica.

4.12.2 PRÁCTICAS Y POLÍTICAS DE RECUPERACIÓN DE CLAVES DE SESIÓN

No estipulado.

5. CONTROLES DE INSTALACIONES, GESTIÓN Y OPERACIONALES

5.1 CONTROLES FÍSICOS

5.1.1 UBICACIÓN FÍSICA Y CONSTRUCCIÓN

Este contenido se detalla en la DPC de la PKI-SAR, en el numeral 5.1.1 denominado Ubicación Física y Construcción, de tal forma remitirse a lo ahí establecido.

5.1.2 ACCESO FÍSICO

Este contenido se detalla en la DPC de la PKI-SAR, en el numeral 5.1.2 denominado Acceso Físico, de tal forma remitirse a lo ahí establecido.

5.1.3 ELECTRICIDAD Y ACONDICIONADOR DE AIRES

Este contenido se detalla en la DPC de la PKI-SAR, en el numeral 5.1.3 denominado Electricidad y Acondicionador de Aires, de tal forma remitirse a lo ahí establecido.

5.1.4 EXPOSICIÓN AL AGUA

Este contenido se detalla en la DPC de la PKI-SAR, en el numeral 5.1.4 denominado Exposición al Agua, de tal forma remitirse a lo ahí establecido.

5.1.5 PREVENCIÓN Y PROTECCIÓN DE INCENDIOS

Este contenido se detalla en la DPC de la PKI-SAR, en el numeral 5.1.5 denominado Prevención y Protección de Incendios, de tal forma remitirse a lo ahí establecido.

5.1.6 EQUIPOS DE ALMACENAMIENTO

Este contenido se detalla en la DPC de la PKI-SAR, en el numeral 5.1.6 denominado Equipos de Almacenamiento, de tal forma remitirse a lo ahí establecido.

5.1.7 MANEJO DE RESIDUOS

Este contenido se detalla en la DPC de la PKI-SAR, en el numeral 5.1.7 denominado Manejo de Residuos, de tal forma remitirse a lo ahí establecido.

5.1.8 COPIAS DE SEGURIDAD FUERA DE LAS INSTALACIONES

Este contenido se detalla en la DPC de la PKI-SAR, en el numeral 5.1.8 denominado Copia de Seguridad Fuera de las Instalaciones, de tal forma remitirse a lo ahí establecido.

5.2 CONTROLES DE PROCEDIMIENTO

5.2.1 ROLES DE PKI-SAR

Este contenido se detalla en la DPC de la PKI-SAR, en el numeral 5.2.1 denominado Roles de PKI-SAR, de tal forma remitirse a lo ahí establecido.

5.2.2 NÚMERO DE PERSONAS REQUERIDAS POR TAREA

Este contenido se detalla en la DPC de la PKI-SAR, En el numeral 5.2.2 denominado Número de Personas Requeridas por Tarea, de tal forma remitirse a lo ahí establecido.

5.2.3 ROLES QUE REQUIEREN SEGREGACIÓN DE FUNCIONES

Este contenido se detalla en la DPC de la PKI-SAR, en el numeral 5.2.3 denominado Roles que Requieren Segregación de Funciones, de tal forma remitirse a lo ahí establecido.

5.3 CONTROLES DE PERSONAL

5.3.1 APTITUD, CONOCIMIENTO Y ACREDITACIÓN DE PROFESIONALES

Este contenido se detalla en la DPC de la PKI-SAR, en el numeral 5.3.1 denominado Aptitud, Conocimiento y Acreditación de Profesionales, de tal forma remitirse a lo ahí establecido.

5.3.2 PROCESO PARA COMPROBACIÓN DE ANTECEDENTES

Este contenido se detalla en la DPC de la PKI-SAR, en el numeral 5.3.2 denominado Proceso para Comprobación de Antecedentes, de tal forma remitirse a lo ahí establecido.

5.3.3 REQUERIMIENTOS DE ENTRENAMIENTO

Este contenido se detalla en la DPC de la PKI-SAR, en el numeral 5.3.3 requerimientos de formación, de tal forma remitirse a lo ahi establecido.

5.3.4 REQUERIMIENTOS Y FRECUENCIA DE REENTRENAMIENTO

Este contenido se detalla en la DPC de la PKI-SAR, en el numeral 5.3.4 denominado Requerimientos y Frecuencia de Reentrenamiento, de tal forma remitirse a lo ahí establecido.

5.3.5 FRECUENCIA Y SECUENCIA DE ROTACIÓN DE OBLIGACIONES

Este contenido se detalla en la DPC de la PKI-SAR, en el numeral 5.3.5 denominado Frecuencia y Secuencia de Rotación de Obligaciones, de tal forma remitirse a lo ahí establecido.

5.3.6 SANCIONES POR ACCIONES NO AUTORIZADAS

Este contenido se detalla en la DPC de la PKI-SAR, en el numeral 5.3.6 denominado Sanciones por Acciones no Autorizadas, de tal forma remitirse a lo ahí establecido.

5.3.7 REQUISITOS DE CONTRATACIÓN DE TERCEROS

Este contenido se detalla en la DPC de la PKI-SAR, en el numeral 5.3.7 denominado Requisitos de Contratación de Terceros, de tal forma remitirse a lo ahí establecido.

5.3.8 DOCUMENTACIÓN PROVISTA AL PERSONAL

Este contenido se detalla en la DPC de la PKI-SAR, en el numeral 5.3.8 denominado Documentación Provista al Personal, de tal forma remitirse a lo ahí establecido.

5.4 PROCEDIMIENTOS DE AUDITORÍA DE REGISTROS

5.4.1 TIPOS DE EVENTOS REGISTRADOS

Este contenido se detalla en la DPC de la PKI-SAR, en el numeral 5.4.1 denominado Tipos de Eventos Registrados, de tal forma remitirse a lo ahí establecido.

5.4.2 FRECUENCIA DE PROCESADO DE REGISTROS

Este contenido se detalla en la DPC de la PKI-SAR, en el numeral 5.4.2 denominado Frecuencia de Procesado de Registros, de tal forma remitirse a lo ahí establecido.

5.4.3 PERÍODO DE RETENCIÓN DE LOS REGISTROS DE AUDITORÍA

Este contenido se detalla en la DPC de la PKI-SAR, en el numeral 5.4.3 denominado Período de Retención de los Registros de Auditoría, de tal forma remitirse a lo ahí establecido.

5.4.4 PROTECCIÓN DE LOS REGISTROS DE AUDITORÍA

Este contenido se detalla en la DPC de la PKI-SAR, en el numeral 5.4.4 denominado Protección de los Registros de Auditoría, de tal forma remitirse a lo ahí establecido.

5.4.5 PROCEDIMIENTOS DE RESPALDO DE LOS REGISTROS DE AUDITORÍA

Este contenido se detalla en la DPC de la PKI-SAR, en el numeral 5.4.5 denominado Procedimientos de Respaldo de los Registros de Auditoría, de tal forma remitirse a lo ahí establecido.

5.4.6 SISTEMA DE RECOLECCIÓN DE REGISTROS

Este contenido se detalla en la DPC de la PKI-SAR, en el numeral 5.4.6 denominado Sistema de Recolección de Registros, de tal forma remitirse a lo ahí establecido.

5.4.7 NOTIFICACIÓN AL SUJETO CAUSANTE DEL EVENTO

No estipulado.

5.4.8 ANÁLISIS DE VULNERABILIDADES

Como establece la DPC de la PKI-SAR, en el numeral 5.4.8 denominado Análisis de Vulnerabilidades, de tal forma remitirse a lo ahí establecido.

5.5 ARCHIVADO DE REGISTROS

5.5.1 TIPO DE EVENTOS ARCHIVADOS

Este contenido se detalla en la DPC de la PKI-SAR, en el numeral 5.5.1 denominado Tipo de Eventos Archivados, de tal forma remitirse a lo ahí establecido.

5.5.2 PERÍODO DE CONSERVACIÓN DE REGISTROS

Este contenido se detalla en la DPC de la PKI-SAR, en el numeral 5.5.2 denominado Período de Conservación de Registros, de tal forma remitirse a lo ahí establecido.

5.5.3 PROTECCIÓN DEL ARCHIVO

Este contenido se detalla en la DPC de la PKI-SAR, en el numeral 5.5.3 denominado Protección del Archivo, de tal forma remitirse a lo ahí establecido.

5.5.4 PROCEDIMIENTOS DE COPIA DE RESPALDO DEL ARCHIVO

Este contenido se detalla en la DPC de la PKI-SAR, en el numeral 5.5.4 denominado Procedimientos de Copia de Respaldo del Archivo, de tal forma remitirse a lo ahí establecido.

5.5.5 REQUISITO PARA EL SELLADO DE TIEMPO DE LOS REGISTROS

Este contenido se detalla en la DPC de la PKI-SAR, en el numeral 5.5.5 denominado Requisito para el Sellado de Tiempo de los Registros, de tal forma remitirse a lo ahí establecido.

5.5.6 PROCEDIMIENTOS PARA OBTENER Y VERIFICAR INFORMACIÓN ARCHIVADA

Este contenido se detalla en la DPC de la PKI-SAR, en el numeral 5.5.6 denominado Procedimientos para Obtener y Verificar Información Archivada, de tal forma remitirse a lo ahí establecido.

5.6 CAMBIO DE CLAVES

Como establece la DPC de la PKI-SAR, en el numeral 5.6 denominado Cambio de Claves, de tal forma remitirse a lo ahí establecido.

5.7 RECUPERACIÓN POR COMPROMISO DE CLAVE O CATÁSTROFE

5.7.1 GESTIÓN DE INCIDENTES Y VULNERABILIDADES

Este contenido se detalla en la DPC de la PKI-SAR, en el numeral 5.7.1 denominado Gestión de Incidentes y Vulnerabilidades, de tal forma remitirse a lo ahí establecido.

5.7.2 ACTUACIÓN ANTE DATOS Y SOFTWARE CORRUPTOS

Este contenido se detalla en la DPC de la PKI-SAR, en el numeral 5.7.2 denominado Actuación Ante Datos y Software Corruptos, de tal forma remitirse a lo ahí establecido.

5.7.3 PROCEDIMIENTO ANTE COMPROMISO DE CLAVE

Como establece la DPC de la PKI-SAR, en el numeral 5.7.3 denominado Procedimiento Ante Compromiso de Clave, de tal forma remitirse a lo ahí establecido.

5.7.4 CONTINUIDAD DEL NEGOCIO DESPUÉS DE UN DESASTRE

Este contenido se detalla en la DPC de la PKI-SAR, en el numeral 5.7.4 denominado Continuidad del Negocio Después de un Desastre, de tal forma remitirse a lo ahí establecido.

5.8 CESE DE UNA AUTORIDAD CERTIFICADORA (AC)

5.8.1 AUTORIDAD DE CERTIFICACIÓN

Este contenido se detalla en la DPC de la PKI-SAR, en el numeral 5.8.1 denominado Autoridad de Certificación, de tal forma remitirse a lo ahí establecido.

5.8.2 AUTORIDAD DE REGISTRO

Este contenido se detalla en la DPC de la PKI-SAR, en el numeral 5.8.2 denominado Autoridad de Registro, de tal forma remitirse a lo ahí establecido.

PKI-SAR, en el numeral 5.8.1 denominado Autoridad de Certificación, de tal forma remitirse a lo ahí establecido.

5.8.3 AUTORIDAD DE REGISTRO

Este contenido se detalla en la DPC de la PKI-SAR, en el numeral 5.8.2 denominado Autoridad de Registro, de tal forma remitirse a lo ahí establecido.

6. CONTROLES DE SEGURIDAD TÉCNICA

6.1 GENERACIÓN E INSTALACIÓN DEL PAR DE CLAVES

6.1.1 GENERACIÓN DEL PAR DE CLAVES

En relación con la generación de las claves del Suscriptor(a), es importante mencionar que la PKI-SAR no genera ni almacena las claves privadas asociadas a los certificados expedidos bajo las presentes PC, debido a que son generadas bajo el exclusivo control del Suscriptor(a).

6.1.2 ENTREGA DE LA LLAVE PRIVADA AL SUSCRIPTOR(A)

No existe ninguna entrega de clave privada en la emisión de los certificados expedidos bajo la presente PC. Las claves privadas asociada a los certificados de persona jurídica son generadas bajo el control exclusivo del Suscriptor(a) y custodiadas en un archivo criptográfico PKCS12 para su uso.

6.1.3 ENTREGA DE LA CLAVE PÚBLICA AL EMISOR DEL CERTIFICADO

La clave pública es generada, junto a la clave privada, en el archivo PKCS12 y es entregada a Suscriptor(a) mediante el envío de un correo electrónico remitido de forma automática desde la AR al correo que proporcionó en el registro de información.

6.1.4 ENTREGA DE LA CLAVE PÚBLICA DE LA AC A LOS TERCEROS QUE CONFÍAN

La clave pública de las CA de PKI-SAR está a disposición de los terceros que confían, en el Repositorio de PKI-SAR (ver apartado 2.1. Repositorio).

6.1.5 TAMAÑO DE LAS CLAVES

El tamaño de las claves de los certificados de persona jurídica es de 2048 bits, el algoritmo utilizado es RSA con SHA256.

6.1.6 PARÁMETROS DE GENERACIÓN DE LA CLAVE PÚBLICA Y ASEGURAMIENTO DE LA CALIDAD

La clave pública de los certificados de persona jurídica de la PKI-SAR está codificada de acuerdo con RFC 3280 y PKCS#1 siendo el algoritmo de generación de claves RSA.

6.1.7 USOS ADMITIDOS DE LA CLAVE (CAMPO KEYUSAGE DE X.509 V3)

Los usos admitidos de la clave para los certificados de persona jurídica vienen dados por el valor de las extensiones Key Usage y Extended Key Usage de los mismos. El contenido de dichas extensiones para cada uno de los tipos de certificados de persona jurídica se puede consultar en el apartado 7.1.2. Extensiones del Certificado del presente documento.

6.2 PROTECCIÓN DE LA CLAVE PRIVADA Y CONTROLES DE INGENIERÍA DE LOS MÓDULOS

6.2.1 ESTÁNDARES PARA LOS MÓDULOS CRIPTOGRÁFICOS

Este contenido se detalla en la DPC de la PKI-SAR, en el numeral 6.2.1 denominado Estándares para los Módulos Criptográficos, de tal forma remitirse a lo ahí establecido.

6.2.2 CONTROL MULTIPERSONA (K DE N) DE LA CLAVE PRIVADA

Las claves privadas de los certificados de persona jurídica no se encuentran bajo control multipersona. El control de dicha clave privada recae enteramente sobre el Suscriptor(a).

6.2.3 RESGUARDO DE LA CLAVE PRIVADA

La custodia de las claves privadas de los certificados de persona jurídica la realizan los Suscriptores(as) de estas.

6.2.4 RESPALDO DE LA CLAVE PRIVADA

En ningún caso se realizan copias de seguridad de las claves privadas de firma de persona jurídica para garantizar el no repudio.

6.2.5 ARCHIVO DE LA CLAVE PRIVADA

Las claves privadas de firma de persona jurídica nunca son archivadas para garantizar el no repudio.

6.2.6 TRANSFERENCIA DE LA CLAVE PRIVADA HACIA O DESDE UN MÓDULO CRIPTOGRÁFICO

En ningún caso es posible transferir las claves privadas de firma de persona jurídica para garantizar el no repudio.

6.2.7 ALMACENAMIENTO DE LA CLAVE PRIVADA EN UN MÓDULO CRIPTOGRÁFICO

Las claves privadas de firma de persona jurídica se generan en un archivo criptográfico PKCS12 en el momento de la generación de los certificados.

6.2.8 MÉTODO DE ACTIVACIÓN DE LA CLAVE PRIVADA

La activación de la clave privada la puede efectuar el Suscriptor(a) de esta mediante el uso de su contraseña de firma (únicamente conocido por el).

6.2.9 MÉTODO DE DESACTIVACIÓN DE LA CLAVE PRIVADA

La desactivación de la clave privada de persona jurídica se realiza mediante solicitud del representante de la Persona Jurídica. Esta desactivación se trata como una revocación del certificado electrónico por lo que se sigue el procedimiento establecido para tal fin.

6.2.10 MÉTODO DE DESTRUCCIÓN DE LA CLAVE PRIVADA

La destrucción de la clave privada debe ser precedida por una revocación del certificado electrónico asociado a la clave, si esta estuviese todavía vigente o una vez agotado su período de uso. La PKI-SAR dispone de un método de destrucción de forma que impida su robo o uso no autorizado.

6.2.11 CLASIFICACIÓN DE LOS MÓDULOS CRIPTOGRÁFICOS

Los módulos criptográficos empleados cumplen el estándar FIPS 140-2 nivel 3.

6.3 OTROS ASPECTOS DE LA ADMINISTRACIÓN DEL PAR DE CLAVES

6.3.1 ARCHIVO DE LA CLAVE PÚBLICA

Este contenido se detalla en la DPC de la PKI-SAR en el numeral 6.3.1 denominado Archivo de la Clave Pública, de tal forma remitirse a lo ahí establecido.

6.3.2 PERÍODOS OPERATIVOS DE LOS CERTIFICADOS Y PERÍODO PARA USO DEL PAR DE CLAVES

El período de validez de los certificados de persona jurídica es no mayor a 3 años desde el momento de emisión de este, de tal forma remitirse a lo ahí establecido.

6.4 DATOS DE ACTIVACIÓN

6.4.1 INSTALACIÓN Y GENERACIÓN DE LOS DATOS DE ACTIVACIÓN

Este contenido se detalla en la DPC de la PKI-SAR, en el numeral 6.4.1 denominado Instalación y Generación de los Datos de Activación, de tal forma remitirse a lo ahí establecido.

6.4.2 PROTECCIÓN PARA DATOS DE ACTIVACIÓN

Este contenido se detalla en la DPC de la PKI-SAR, en el numeral 6.4.2 denominado Protección para Datos de Activación.

6.4.3 OTROS ASPECTOS REFERENTES A LOS DATOS DE ACTIVACIÓN

No estipulado.

6.5 CONTROLES DE SEGURIDAD INFORMÁTICA

6.5.1 REQUERIMIENTOS TÉCNICOS ESPECÍFICOS DE SEGURIDAD INFORMÁTICA

Este contenido se detalla en la DPC de la PKI-SAR, en el numeral 6.5.1 denominado Requerimientos Técnicos Específicos de Seguridad Informática, de tal forma remitirse a lo ahí establecido.

6.5.2 EVALUACIÓN DEL NIVEL DE SEGURIDAD INFORMÁTICA

Este contenido se detalla en la DPC de la PKI-SAR, en el numeral 6.5.2 denominado Evaluación del Nivel de Seguridad Informática, de tal forma remitirse a lo ahí establecido.

6.6 CONTROLES TÉCNICOS DE CICLO DE VIDA

6.6.1 CONTROLES DE DESARROLLO DE SISTEMA

Este contenido se detalla en la DPC de la PKI-SAR, en el numeral 6.6.1 denominado Controles de Desarrollo de Sistema, de tal forma remitirse a lo ahí establecido.

6.6.2 CONTROLES DE ADMINISTRACIÓN DE SEGURIDAD

Este contenido se detalla en la DPC de la PKI-SAR, en el numeral 6.6.2 denominado Controles de Administración de Seguridad, de tal forma remitirse a lo ahí establecido.

6.6.3 CONTROLES DE SEGURIDAD DEL CICLO DE VIDA

Este contenido se detalla en la DPC de la PKI-SAR, en el numeral 6.6.3 denominado Controles de Seguridad del Ciclo de Vida, de tal forma remitirse a lo ahí establecido.

6.7 CONTROLES DE SEGURIDAD DE REDES

Este contenido se detalla en la DPC de la PKI-SAR, en el numeral 6.7 denominado Controles de Seguridad de Redes, de tal forma remitirse a lo ahí establecido.

6.8 SELLADO DE TIEMPO

Este contenido se detalla en la DPC de la PKI-SAR, en el numeral 6.8 denominado Sellado de Tiempo, de tal forma remitirse a lo ahí establecido.

6.9 OTROS CONTROLES ADICIONALES

6.9.1 CONTROL DE LA CAPACIDAD DE PRESTACIÓN DE LOS SERVICIOS

Este contenido se detalla en la DPC de la PKI-SAR, en el numeral 6.9.1 denominado Control de la Capacidad de Prestación de los Servicios, de tal forma remitirse a lo ahí establecido.

6.9.2 CONTROL DE DESARROLLO DE SISTEMAS Y APLICACIONES INFORMÁTICAS

Este contenido se detalla en la DPC de la PKI-SAR, en el numeral 6.9.2 denominado Control de Desarrollo de Sistemas y Aplicaciones Informáticas, de tal forma remitirse a lo ahí establecido.

7. PERFILES DE CERTIFICADOS OCSP Y CRLS

7.1 PERFIL DE CERTIFICADO

7.1.1 NÚMERO DE VERSIÓN

PKI-SAR es compatible con certificados X.509 versión 2 (X.509 v2).

7.1.2 EXTENSIONES DEL CERTIFICADO

A continuación, se detalla el contenido del certificado de Firma Electrónica Avanzada de Persona Jurídica:

Contenido del certificado de firma electrónica avanzada de persona jurídica				
	Atributo	Valor	Obligatorio	Crítica
Version	-	3	Si	-
Serial Number	-	<Número entero, mayor a cero (0) y aleatorio de al menos 20 bytes>	Si	-
Signature	Algorithm	Sha256WithRSAEncryption	Si	-
Issuer	CN	AUTORIDAD SUBORDINADA DEL SAR	Si	-
	O	SERVICIO DE ADMINISTRACION DE RENTAS	Si	-
	C	HN	Si	-
Validity	Not After	<fecha emisión>	Si	-
	Not Before	<fecha expiración>	Si	-
Subject	C	HN	Si	-
	O	PERSONA JURIDICA	Si	
	OU	FIRMA ELECTRONICA	Si	
	CN	CN=[F] NOMBRE PERSONA JURIDICA<Nombre descriptivo de la persona jurídica, asegurando que dicho nombre tenga sentido y no dé lugar a ambigüedad>	Si	
	Description	REGISTRO TRIBUTARIO NACIONAL	Si	-
	BusinessCategory	<Denominación o razón social>	Si	-
Subject Public Key Info	Algorithm	RSA	Si	-

A continuación, se detalla el contenido de las extensiones más significativas de los certificados de Persona Jurídica:

Extensión del certificado de firma electrónica avanzada de persona jurídica				
Nombre	Atributo	Valor	Obligatorio	Crítica
Authority Key Identifier	-	<Resumen SHA-1 (160 bits) de la llave pública del campo Subject Public Key Info del emisor>	Si	No
Authority Key Identifier	-	<Resumen SHA-1 (160 bits) de la llave pública del campo Subject Public Key Info del emisor>	Si	No
Subject Key Identifier	-	<Resumen SHA-1 (160 bits) de la llave pública del campo Subject Public Key Info del emisor>	Si	No
Key Usage	-	digitalSignature, nonRepudiation	Si	Si
Extended Key Usage	-	-	Si	No
Certificate Policies	policyIdentifier (OID)	1.3.6.1.4.1.52089.2.3	Si	No
	cPSuri	URL: https://www.sar.gob.hn/firmaelectronica/		
Basic Constraints	Subject Type	End Entity	Si	Si
	Path Length Constraint	None	-	-
CRL Distribution Points	Distribution Point Name (URI)	<http://pki.sar.gob.hn/crlsar/crl.crl>	Si	
Authority Informatio n Access	cAIssuers (URI)	http://pki.sar.gob.hn/crlsar/casub.crt	Si	
	OCSP (URI)	http://ocsp2.sar.gob.hn/CryptosecOpenKey/va_ser vice		

7.1.3 IDENTIFICADOR DE OBJETO (OID) DE LOS ALGORITMOS

Identificador de Objeto (OID) de los algoritmos Criptográficos utilizando SHA256 with RSA Encryption es 1.2.840.113549.1.1.11

7.1.4 FORMATO DE NOMBRES

Los certificados emitidos por la PKI-SAR contienen el distinguished name X.500 del emisor y del titular del certificado en los campos issuer name y subject name respectivamente.

7.1.5 RESTRICCIÓN DE LOS NOMBRES

Los nombres contenidos en los certificados están restringidos a distinguished names X.500, que son únicos y no ambiguos.

7.1.6 IDENTIFICADOR DE OBJETO (OID) DE LAS POLÍTICAS DE CERTIFICACIÓN

El identificador de objeto de la Política de Certificado de Firma Electrónica Avanzada de Persona Jurídica es la definida en el apartado 1.2 denominado Nombre del Documento e Identificación de la PC.

7.1.7 USO DE LA EXTENSIÓN "POLICYCONSTRAINTS"

La extensión Policy Constrains del certificado raíz de la AC no es utilizado.

7.1.8 SINTAXIS Y SEMÁNTICA DE LOS "POLICYQUALIFIER"

La extensión Certificate Policies contiene los siguientes Policy Qualifiers:

- URL CPS: contiene la URL, la DPC y la PC que rigen el certificado.

- Notice Reference: Nota de texto que se despliega en la pantalla, a instancia de una aplicación o persona, cuando un tercero verifica el certificado.

En el campo Notice Reference se incluye un texto con información básica sobre el certificado y las políticas a que está sujeto.

7.1.9 TRATAMIENTO SEMÁNTICO PARA LA EXTENSIÓN CRÍTICA "CERTIFICATEPOLICIES"

La extensión "CertificatePolicies" incluye el campo OID de política, que identifica.

7.2 PERFIL CRL

7.2.1 NÚMERO DE VERSIÓN

El perfil de las CRL es conforme con el estándar X.509 versión 3.

7.2.2 CRL Y EXTENSIONES

El perfil de la CRL sigue la siguiente estructura:

Campo y extensión	Valor
Versión	V2
Algoritmo de firma	SHA256RSA para jerarquía AC RAIZ PKI-SAR
Número de CRL	Valor incremental
Emisor	Subject del PKI-SAR
Fecha de emisión	Tiempo de emisión
Fecha próxima de actualización	Fecha de emisión + 24 horas (Salvo la ARL que es fecha de emisión + 1 año)
Identificador de la clave de autoridad	Hash de la clave de la PKI-SAR
Punto de distribución	URL del punto de distribución
Certificados revocados	Lista de certificados revocados, conteniendo número de serie y fecha de revocación

7.3 PERFIL DE OCSP

7.3.1 NÚMERO DE VERSIÓN

La Autoridad de Validación admite peticiones firmadas y las extensiones definidas en RFC 2560.

7.3.2 EXTENSIONES OCSP

Este contenido se detalla en la DPC de la PKI-SAR, en el numeral 7.3.2 denomina extensiones OCSP, de tal forma remitirse a lo ahí establecido.

8. AUDITORÍAS DE CUMPLIMIENTO Y OTROS CONTROLES

8.1 FRECUENCIA O CIRCUNSTANCIAS DE LOS CONTROLES PARA CADA AUTORIDAD

Este contenido se detalla en la DPC de la PKI-SAR, en el numeral 8.1 denominado Frecuencia o Circunstancias de los Controles para Cada Autoridad, de tal forma remitirse a lo ahí establecido.

8.2 IDENTIFICACIÓN/CUALIFICACIÓN DEL AUDITOR

Este contenido se detalla en la DPC de la PKI-SAR, en el numeral 8.2 denominado Identificación/Cualificación del Auditor, de tal forma remitirse a lo ahí establecido.

8.3 RELACIÓN ENTRE EL AUDITOR Y LA AUTORIDAD AUDITADA

Este contenido se detalla en la DPC de la PKI-SAR, en el numeral 8.3 denominado Relación Entre el Auditor y la Autoridad Auditada, de tal forma remitirse a lo ahí establecido.

8.4 ASPECTOS CUBIERTOS POR LOS CONTROLES

Este contenido se detalla en la DPC de la PKI-SAR, en el numeral 8.4 denominado Aspectos Cubiertos por los Controles, de tal forma remitirse a lo ahí establecido.

8.5 TOMA DE DECISIONES FRENTE A LA DETECCIÓN DE DEFICIENCIAS

Este contenido se detalla en la DPC de la PKI-SAR, en el numeral 8.5 denominado Toma de Decisiones Frente a la Detección de Deficiencias, de tal forma remitirse a lo ahí establecido.

8.6 COMUNICACIÓN DE RESULTADOS

Este contenido se detalla en la DPC de la PKI-SAR, en el numeral 8.6 denominado Comunicación de Resultados, de tal forma remitirse a lo ahí establecido.

9. OTROS ASPECTOS LEGALES Y DE ACTIVIDAD

9.1 TARIFAS

9.1.1 TARIFAS PARA EMISIÓN O RENOVACIÓN DE CERTIFICADO

Las tarifas de emisión y renovación de cada certificado de Firma Electrónica avanzada de Persona Jurídica, tendrá una tarifa plana, que dependerá del tamaño de contribuyente que se trate, según el estudio realizado por el Departamento de Estudios Fiscales de Servicio de Administración de Rentas (SAR).

9.1.2 TARIFAS PARA ACCESO A CERTIFICADOS

Grandes contribuyentes: L. 1,500.00
Medianos Contribuyentes: L.750.00
Pequeños contribuyentes: L.350.00

9.1.3 TARIFAS PARA ACCESO A INFORMACIÓN DE ESTADO O REVOCACIÓN

La PKI-SAR ofrece los servicios de información del estado de los certificados a través de CRL o del OCSP de forma gratuita.

9.1.4 TARIFAS PARA OTROS SERVICIOS

Este contenido se detalla en la DPC de la PKI-SAR, en el numeral 9.1.4 denominado Tarifas para Otros Servicios, de tal forma remitirse a lo ahí establecido.

9.1.5 POLÍTICA DE REEMBOLSO

La Administración Tributaria no aplicará ninguna política de reembolso. Los Obligados Tributarios conocerán los términos y condiciones del certificado de Firma electrónica.

9.2 RESPONSABILIDADES ECONÓMICAS

9.2.1 SEGURO DE RESPONSABILIDAD CIVIL

Este contenido se detalla en la DPC de la PKI-SAR, en el numeral 9.2.1 denominado Seguro de Responsabilidad Civil, de tal forma remitirse a lo ahí establecido.

9.2.2 OTROS ACTIVOS

No estipulado.

9.2.3 SEGUROS Y GARANTÍAS PARA ENTIDADES FINALES

No estipulado.

9.3 CONFIDENCIALIDAD DE LA INFORMACIÓN

Este contenido se detalla en la DPC de la PKI-SAR, en el numeral 9.3 denominado Confidencialidad de la Información, de tal forma remitirse a lo ahí establecido.

9.3.1 ALCANCE DE LA INFORMACIÓN CONFIDENCIAL

Este contenido se detalla en la DPC de la PKI-SAR, en el numeral 9.3.1 denominado Alcance de la Información Confidencial, de tal forma remitirse a lo ahí establecido.

9.3.2 INFORMACIÓN NO CONFIDENCIAL

Este contenido se detalla en la DPC de la PKI-SAR, en el numeral 9.3.2 denominado Información no Confidencial, de tal forma remitirse a lo ahí establecido.

9.3.3 RESPONSABILIDAD DE PROTEGER LA INFORMACIÓN CONFIDENCIAL

Como establece la DPC de la PKI-SAR, en el numeral 9.3.3 denominado Responsabilidad de Proteger la Información Confidencial, de tal forma remitirse a lo ahí establecido.

9.4 PROTECCIÓN DE LA INFORMACIÓN PERSONAL

Este contenido se detalla en la DPC de la PKI-SAR, en el numeral 9.4 denominado Protección de la Información Personal, de tal forma remitirse a lo ahí establecido.

9.5 DERECHOS DE PROPIEDAD INTELECTUAL

Este contenido se detalla en la DPC de la PKI-SAR, en el numeral 9.5 denominado Derechos de Propiedad Intelectual, de tal forma remitirse a lo ahí establecido.

9.6 OBLIGACIONES Y GARANTÍAS

9.6.1 OBLIGACIONES DE LA AC

Este contenido se detalla en la DPC de la PKI-SAR, en el numeral 9.6.1 denominado Obligaciones de las AC, de tal forma remitirse a lo ahí establecido.

9.6.2 OBLIGACIONES DE LA AR

Este contenido se detalla en la DPC de la PKI-SAR, en el numeral 9.6.2 denominado Obligaciones de la AR, de tal forma remitirse a lo ahí establecido.

9.6.3 OBLIGACIONES DE LOS SUSCRIPTORES(AS) DE LOS CERTIFICADOS

Este contenido se detalla en la DPC de la PKI-SAR, en el numeral 9.6.3 denominado Obligaciones de los Suscriptores(as) de los Certificados, de tal forma remitirse a lo ahí establecido.

9.6.4 OBLIGACIONES DE LOS TERCEROS QUE CONFÍAN O ACEPTEN LOS CERTIFICADOS

Este contenido se detalla en la DPC de la PKI-SAR, en el numeral 9.6.4 denominado Obligaciones de los Terceros que Confían o Acepten los Certificados, de tal forma remitirse a lo ahí establecido.

9.6.5 EXENCIÓN DE RESPONSABILIDADES

Este contenido se detalla en la DPC de la PKI-SAR, en el numeral 9.7 denominado Exención de Responsabilidades, de tal forma remitirse a lo ahí establecido.

9.6.6 LIMITACIONES DE LAS RESPONSABILIDADES

Este contenido se detalla en la DPC de la PKI-SAR, en el numeral 9.8 denominado Limitaciones de las Responsabilidades, de tal forma remitirse a lo ahí establecido.

9.7 INDEMNIZACIONES

Este contenido se detalla en la DPC de la PKI-SAR, en el numeral 9.9 denominado Indemnizaciones, de tal forma remitirse a lo ahí establecido.

9.7.1 INDEMNIZACIONES DE LA CA

No estipulado.

9.7.2 INDEMNIZACIONES DE LOS SUSCRIPTORES(AS)

No estipulado.

9.7.3 INDEMNIZACIONES DE LAS PARTES QUE CONFÍAN

No estipulado.

9.8 PERÍODO DE VALIDEZ DE ESTE DOCUMENTO

9.8.1 PERÍODO

El período de vigencia de esta PC inicia desde el momento de su publicación en el repositorio de PKI-SAR.

9.8.2 TERMINACIÓN DE LA DPC

Al emitir una nueva versión, esta PC es sustituida en su totalidad, sin importar la trascendencia de los cambios realizados.

9.8.3 EFECTOS DE LA TERMINACIÓN

Las obligaciones y restricciones detalladas en esta PC, estipuladas con respecto a auditorías, información confidencial, obligaciones y responsabilidades de la PKI-SAR, nacidas bajo su vigencia, subsisten tras su renovación o derogación por una nueva versión en todo en lo que no se oponga a ésta.

9.9 NOTIFICACIONES INDIVIDUALES Y COMUNICACIONES CON LOS PARTICIPANTES

Como establece la DPC de la PKI-SAR, en el numeral 9.11 denominado Notificaciones Individuales y Comunicaciones con los Participantes, de tal forma remitirse a lo ahí establecido.

9.10 MODIFICACIONES DE ESTE DOCUMENTO

9.10.1 PROCEDIMIENTO PARA LAS MODIFICACIONES

Este contenido se detalla en la DPC de la PKI-SAR, en el numeral 9.12.1 denominado Procedimiento para las Modificaciones, de tal forma remitirse a lo ahí establecido.

9.10.2 PERÍODO Y MECANISMO DE NOTIFICACIÓN

Este contenido se detalla en la DPC de la PKI-SAR, en el numeral 9.12.2 denominado Período y Mecanismo de Notificación, de tal forma remitirse a lo ahí establecido.

9.10.3 CIRCUNSTANCIAS EN EL QUE EL OID DEBE SER CAMBIADO

Este contenido se detalla en la DPC de la PKI-SAR, en el numeral 9.12.3 denominado Circunstancias Bajo las Cuales debe Cambiarse un OID, de tal forma remitirse a lo ahí establecido.

9.11 RESOLUCIÓN DE CONFLICTOS

Este contenido se detalla en la DPC de la PKI-SAR, en el numeral 9.13 denominado Resolución de Conflictos, de tal forma remitirse a lo ahí establecido.

9.12 NORMATIVA APLICABLE

Este contenido se detalla en la DPC de la PKI-SAR, en el numeral 9.14 denominado Normativa Aplicable, de tal forma remitirse a lo ahí establecido.

9.13 CUMPLIMIENTO DE LA LEGISLACIÓN APLICABLE

Este contenido se detalla en la DPC de la PKI-SAR, en el numeral 9.15 denominado Cumplimiento de la Legislación Aplicable, de tal forma remitirse a lo ahí establecido.

9.14 ESTIPULACIONES MISCELÁNEAS

9.14.1 ACEPTACIÓN DE LA DPC

Todos los Terceros que Confían, aceptan en su totalidad el contenido de la última versión de la DPC y de esta PC.

9.14.2 RESOLUCIÓN DE CONFLICTOS EN LA VÍA JUDICIAL

Este contenido se detalla en la DPC de la PKI-SAR, en el numeral 19.16.2 denominado Resolución de Conflictos en la Vía Judicial, de tal forma remitirse a lo ahí establecido, de tal forma remitirse a lo ahí establecido.

9.15 OTRAS ESTIPULACIONES

No se consideran otras estipulaciones.