Secretaría de Administración

ACUERDO NÚMERO SAR-466-2024
Tegucigalpa, M. D.C., 06 de septiembre de 2024

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

CONSIDERANDO: Que mediante el Artículo 195 del Decreto Legislativo número 170-2016 de fecha quince de diciembre del dos mil dieciséis que contiene el Código Tributario, se 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 ADMINISTRACIÓN DE RENTAS (SAR)**, mediante **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…, 3) Aprobar las políticas institucionales.

CONSIDERANDO: Que mediante Acuerdo Ejecutivo No. 23-2024 de fecha 18 de enero del 2024 se nombró al ciudadano **CHRISTIAN DAVID DUARTE CHAVEZ** 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 MARTÍNEZ**, en el cargo de **SECRETARIA GENERAL** del Servicio de Administración de Rentas (SAR).

CONSIDERANDO: Que los órganos administrativos desarrollarán su actividad 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 economía, celeridad y eficacia, a fin de lograr una pronta y efectiva satisfacción del interés general.

CONSIDERANDO: Que es necesario establecer las Políticas de Certificación de Firma Electrónica Avanzada de Persona Natural, que rigen el funcionamiento y operación de la infraestructura de la Clave Pública del Servicio de Administración de Rentas, desde la descripción del procedimiento para la emisión y gestión de certificados de firma electrónica hasta garantizar que los mismos sean reconocidos y aceptados de acuerdo con los estándares internacionales, jurídicos y técnicos a nivel nacional.

CONSIDERANDO: Que los actos de los órganos de la Administración Pública adoptarán la forma de Decretos, Acuerdos, Resoluciones o Providencias.

POR TANTO: En el uso de las facultades que la Ley le confiere y en aplicación a lo establecido en los Artículos 351 y 361 de la Constitución de la República; 195, 197 numeral 1), y 199 numerales 1), 6) y 13) del Código Tributario; 7, 116, 118 y 122 de la Ley General de Administración Pública; 19 y 30 de la Ley de Procedimiento Administrativo; Acuerdo Ejecutivo 01-2017; Acuerdo Ejecutivo No. 23-2024; Acuerdo Ejecutivo No. 4352022, y demás disposiciones legales aplicables.

ACUERDA:

PRIMERO: Aprobar de la Política de Certificación de Certificado de Firma Electrónica Avanzada de Persona Natural con código POL-GIF-GGI-NDP-021-V1, versión 1.0.

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

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

CHRISTIAN DAVID DUARTE CHAVEZ
DIRECTOR EJECUTIVO

NIDIA SARAIH BERRIOS MARTINEZ
SECRETARIA GENERAL

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

POL-GIF-GGI-NDP-021-V1

SAR

SERVICIO DE ADMINISTRACIÓN DE RENTAS

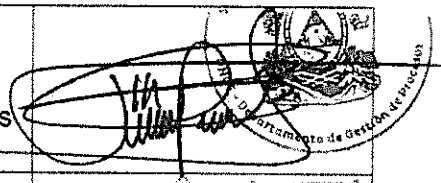
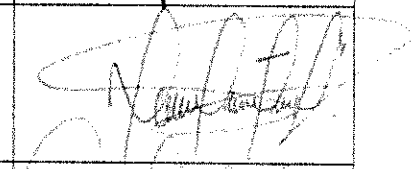
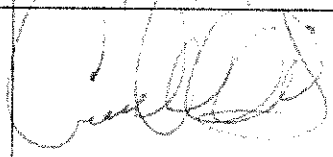
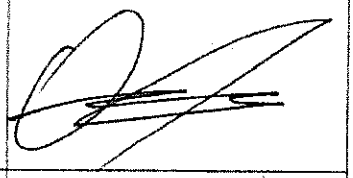
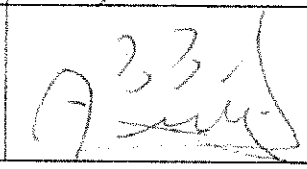
DIRECCIÓN EJECUTIVA

SECRETAÍA GENERAL

Septiembre 2024

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

RUBRO	CARGO	FIRMA
APROBADO POR:	**Lic. Christian David Duarte Chávez** Director Ejecutivo	
REVISADO POR:	**Abg. Nidia Sarahí Berrios Martínez** Secretaría General	
	Ing. Diana Orestila Cárcamo Rodríguez 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 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 de Política de Certificado de Firma Electrónica Avanzada de Persona Natural, estipula el funcionamiento y operaciones de la Infraestructura de Clave Pública (en adelante PKI) del Servicio de Administración de Rentas (en adelante, el 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 Internet Engineering Task Force (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 naturales, así como a los terceros que confían en los certificados y servicios de Sellado de Tiempo brindados por el SAR.

1.1. VISIÓN GENERAL

1.1.1. CONTROL DEL DOCUMENTO

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.

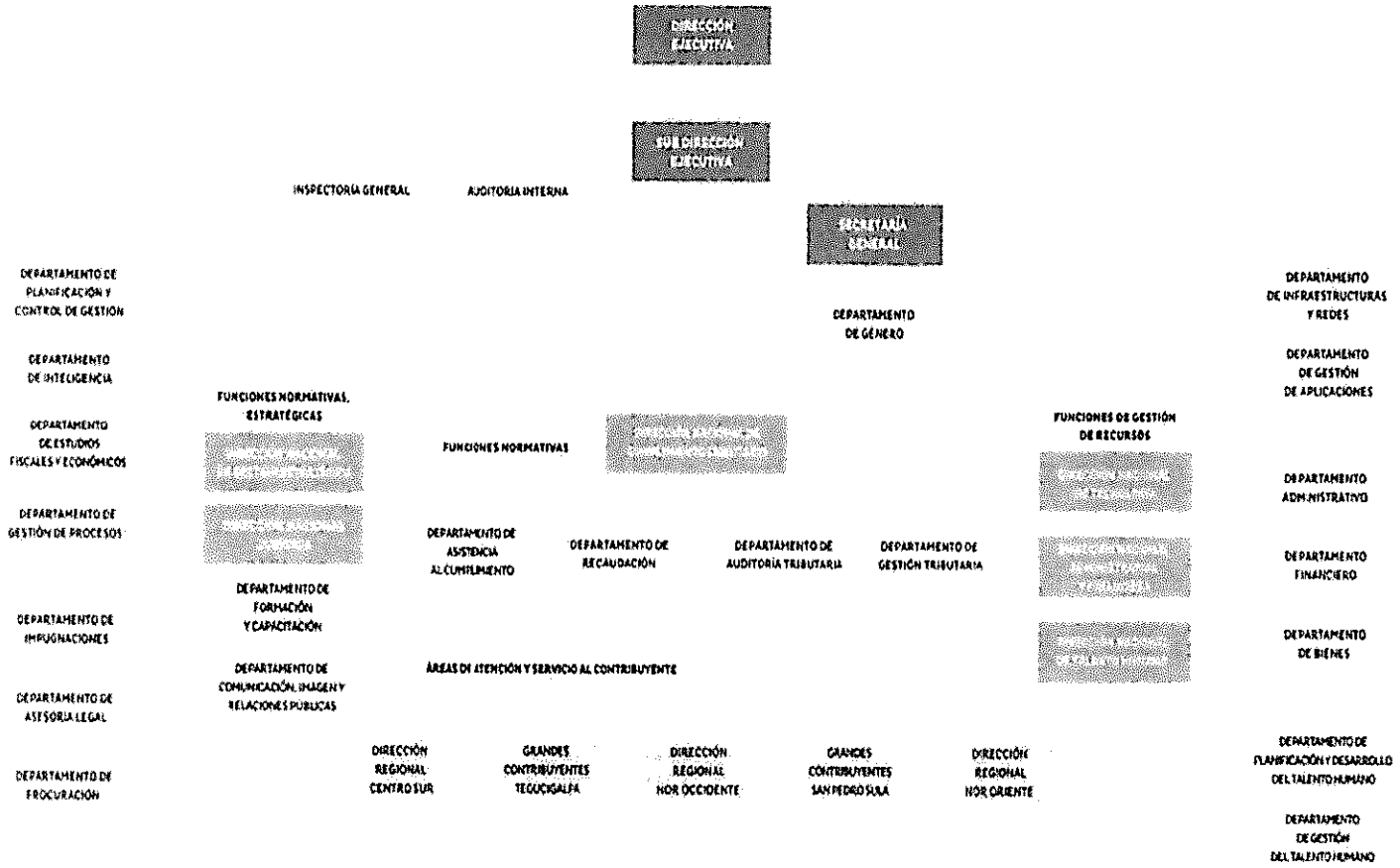
1.1.3. EJES TRANSVERSALES VINCULADO AL DOCUMENTO

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 las Políticas de Certificación de Certificado de Firma Electrónica Avanzada de Persona Natural, las que rigen el funcionamiento y operación de la Infraestructura de Clave Pública de Servicio de Administración de Rentas (PKI-SAR).

1.1.8. ALCANCE

Esta política consiste en detallar que todos los certificados de firma electrónica emitidos por la entidad responsable sean aceptados, para cumplir con los requisitos del estándar RFC 3647 versión 3. Se 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 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 por la PKI-SAR.

b. Los cambios y/o modificaciones que experimente el marco normativo nacional, prevalece 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, deben ser regulados por las disposiciones legales que apliquen.

d. Esta PC establece los requisitos particulares de los certificados para persona natural 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 1.1.9 Referencia técnica.

e.

1.1.10. EXCLUSIONES

Este documento ha sido diseñado con base en las recomendaciones de la RFC 7382 (Modelo de Declaración de Prácticas de Certificación (CPS) para la PKI de recursos (RPKI). Las secciones que están determinadas como "No estipulado" en el Modelo de Declaración de Prácticas de Certificación (CPS) para la PKI de recursos (RPKI), no tienen inherencia en nuestro marco de cumplimiento.

1.1.11. MARCO NORMATIVO

Identificación de norma (Decreto, Acuerdo o Resolución)	Fecha de vigencia	Referencia específica
Decreto No.149 -2013 y sus reformas	2013	Ley Sobre Firmas Electrónicas
Acuerdo Ejecutivo No.41-2014	2015	Reglamento de la Ley Sobre Firmas Electrónicas
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 3 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 DPC

El nombre de este documento es "Política de Certificación de Firma Electrónica Avanzada de Persona Natural", **versión 1,** la cual entra en vigencia a partir de su publicación, y debe de ser sustituida al momento de la elaboración y publicación de una nueva versión.

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

El Indicador de Objeto (OID) correspondiente a este documento es el siguiente: 1.3.6.1.4.1.52089.2.2

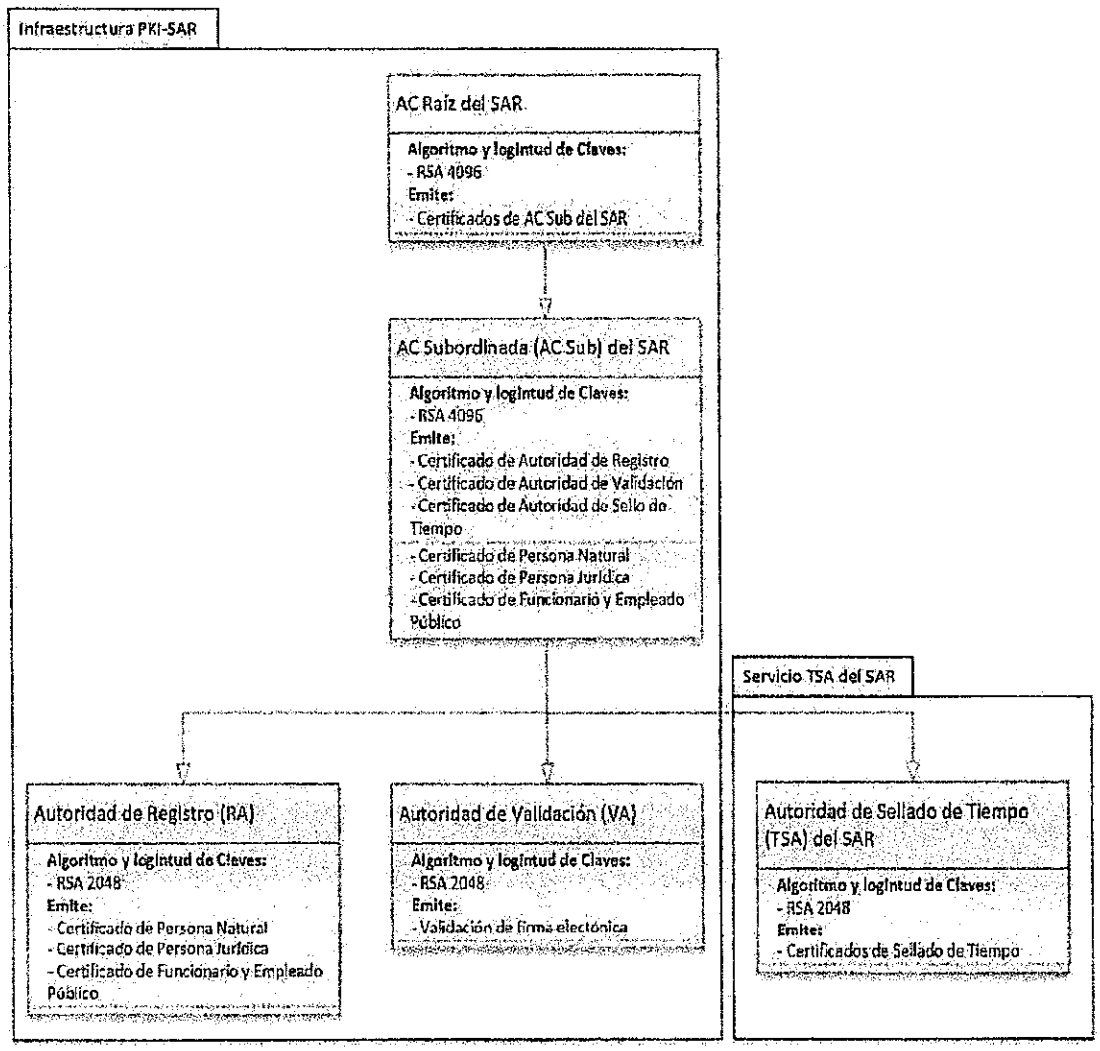
1.3. PARTICIPANTES DE LA PKI

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

1. Autoridad de Certificación (AC).
2. Autoridad de Registro (AR).

3. Autoridad de Validación (AV).
4. Autoridad de Sellado de Tiempo (AST).
5. Comité de Firma Electrónica.
6. Solicitantes y Suscriptores de certificados.
7. Terceros que confían en los certificados de la PKI del Servicio de Administración de Rentas.
8. Autoridad Administrativa Competente (AAC).
9. Prestador de Servicios de Certificación (PSC).

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



1.3.1. AUTORIDADES DE CERTIFICACIÓN (AC)

De acuerdo a lo señalado en el artículo 23 del Reglamento de la Ley Sobre Firmas Electrónicas, pueden actuar como Autoridad de 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 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, regida bajo el Certificado Raíz. Este consiste en un certificado auto-firmado mediante el que se inicia la cadena de confianza, el cual debe permanecer fuera de línea una vez se realice la ceremonia de llaves y se generen 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				
Nombre	**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	-

Contenido del certificado Autoridad Certificadora Raíz del SAR				
Nombre	Atributo	Valor	Obligatorio	Crítica
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 del Servicio de Administración de Rentas implementa una AC Subordinada, siendo esta la que se encuentra en el siguiente eslabón de jerarquía de la AC Raíz; por tanto, la AC 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 Number	-	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	-

Contenido del certificado Autoridad Subordinada del SAR				
Nombre	Atributo	Valor	Obligatorio	Crítica
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 (RA) 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 esta 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.

1.3.5. AUTORIDAD DE VALIDACIÓN (AV)

La Autoridad de Validación (AV) debe determinar de forma online el estado actual de cualquier certificado emitido por el componente AC Subordinada, a través del protocolo OCSP, de acuerdo con los 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 Certificados 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 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, esta 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 DE CERTIFICADOS

Los solicitantes de certificados son definidos por la DPC de la PKI-SAR. Dentro del contexto de esta PC, los Suscriptores y solicitantes de "Certificado de Firma Electrónica Avanzada de Persona Natural" es cualquier persona natural que posea un Documento Nacional de Identidad de Honduras o una persona extranjera residente en Honduras que presente su Carnet de Residencia, o 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 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 actividades siguientes:

- Emitir certificados en relación con las firmas electrónicas certificadas de, persona natural o persona jurídica;
- 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 certificadas;
- Ofrecer o facilitar los servicios de registro y estampado cronológico en la generación, transmisión y recepción de mensajes de datos; y,
- Ofrecer los servicios de archivo y conservación de mensajes de datos.

Las personas naturales, y las personas jurídicas, tanto públicas como privadas, pueden actuar como Autoridad Certificadora o Prestador de Servicios de Certificación (PSC), ; conforme las condiciones siguientes:

- Contar con la capacidad económica y financiera suficiente para prestar los servicios autorizados como autoridad certificadora, así como con el Recursos Humanos 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; 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;
- Seguro;
- 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 requieren, en 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 Certificado de Persona Natural es la certificación electrónica expedida por la PKI-SAR, que vincula a un Suscriptor con unos datos de verificación de firma y confirma su identidad. Los certificados regulados por la presente PC, sólo debe utilizarse con el propósito de firma electrónica de persona natural.

1.4.2. PROHIBICIONES DE USO DE LOS CERTIFICADOS

Los Certificados de Persona Natural no deben 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 Natural son establecidos por el Servicio de Administración de Rentas a través de su 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 DE LA POLÍTICA DE CERTIFICACIÓN DE PERSONA NATURAL

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

1.5.3. RESPONSABLE DE LAS MODIFICACIONES A LA PC

El SAR dispone, dentro de sus competencias como PSC, de capacidad para especificar, revisar y aprobar los procedimientos de revisión y modificaciones de la Política de Certificación de Persona Natural.

Todas las modificaciones realizadas a la PC deben ser publicadas en el sitio web de Servicio de Administración de Rentas, en la dirección https://sar.gob.hn/firmaelectronica/. En caso de existir disconformidad de las modificaciones por parte de algún Suscriptor, 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 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, envíenos 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 TEMINOS

- **Autenticación:** Proceso de intento de verificar la identidad digital de los Solicitantes o Suscriptores de un certificado de la República de Honduras, de este modo la PKI-SAR se asegura de que los Solicitantes o Suscriptores 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, 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 Raíz y CA Subordinada.

- **Identificación:** Implica la acción y efecto de identificar, que es reconocer a un solicitante o Suscriptor de certificado en la República de Honduras.

- **FIPS 140-2:** Es el estándar para validar la eficacia de hardware criptográfico.

- **No Repudio:** El titular y el receptor de la firma electrónica no puede repudiar o desconocer un mensaje de datos que ha sido firmado electrónicamente, dadas las caracteriza de autenticidad e integridad, que garantizan la firma electrónica avanzada.

- **Oficina de Registro:** Lugar designado por la PKI-SAR para la generación del certificado de persona natural, previa validación del proceso de generación del mismo.

- **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** Archivo para el almacenamiento de muchos objetos criptográficos en un solo archivo.

Software PKCS12:

- **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:** Entidad final para quien se han emitido certificados.
- **Tercero que confía:** Individuo o entidad distinta del Suscriptor que decide confiar en los certificados electrónicos emitidos por la PKI-SAR.
- **Unicidad:** Calidad de único o el hecho de las propiedades de cierto objeto definido hace que éste sea único.
- **Validación:** Proceso mediante el cual se verifica la certeza de los datos provistos por el solicitante; en el caso de certificados, corresponde a la verificación del estado de estos.

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.
- IETF Internet Engineering Task Force - Es la principal organización de desarrollo de estándares para internet.
- **IEC:** International Electrotechnical Commission – Comisión Electrotécnica Internacional.
- 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 35dentificación 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.
- **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 Persona Natural 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 Natural y sus modificaciones son de uso publicado consecuentemente al momento de su aprobación. Dicha documentación es publicada en el sitio web al que se hace mención en el numeral 2.1. denominado repositorios.

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

2.4. CONTROLES DE ACCESO A LOS REPOSITORIOS

Todos los repositorios anteriormente citados son de acceso libre para la consulta y descarga de la información. Asimismo, la PKI-SAR establece 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 de certificados requieren de un Distinguished Name el cual debe cumplir con el estándar RFC 5280 "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 natural.

Campo	Valor	Descripción
C	HN	País
O	<Nombre de la persona jurídica>	Organización
OU	FIRMA ELECTRÓNICA	Unidad Organizacional
CN	CN=[F] NOMBRE <apellidos nombre> – DNI <documento nacional de identidad/pasaporte>	Nombre Común

3.1.2. NECESIDAD DE QUE LOS NOMBRES SEAN SIGNIFICATIVOS

Se recomienda que los nombres de los Suscriptores de los certificados sean significativos para todos los casos. La descripción de los atributos asociados al Suscriptor 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 de certificado.

3.1.4. UNICIDAD DE LOS NOMBRES

La agrupación del Nombre Distintivo (DN) y el contenido de la extensión Policy Indentifier debe ser único y no confuso. El uso del número de identidad o pasaporte 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 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 natural expedidos bajo las presente PC. Las claves privadas son generadas bajo el exclusivo control del firmante.

Para la expedición de los certificados para las personas naturales, se requiere que el solicitante genere la clave privada en el sistema del PKI-SAR, después de haber sido registrado en el mismo y 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

Este punto no es aplicable a esta PC. Los certificados expedidos bajo la presente política no incorporan información de la relación de una persona natural con ninguna organización.

3.2.3. AUTENTICACIÓN DE LA IDENTIDAD DE LA PERSONA FÍSICA SOLICITANTE

Los Solicitantes de Certificados de Persona Natural deben comparecer físicamente para formalizar el procedimiento de confirmación de identidad personal, presentándose ante una persona con capacidad para realizar la acreditación en una Oficina de Registro autorizada, con los siguientes medios de identificación:

- Ciudadanos hondureños: Documento Nacional de Identificación (DNI), en los que conste su número de DNI.
- Extranjeros: Tarjeta de Identificación de Extranjeros (donde conste el DNI) o Documento oficial de Pasaporte.

El encargado de acreditación verifica que los documentos aportados cumplan todos los requisitos para confirmar la identidad del solicitante.

La PKI-SAR desarrolla controles oportunos para comprobar la veracidad de la información incluida en el certificado.

3.2.4. INFORMACIÓN NO VERIFICADA SOBRE EL SOLICITANTE

Este numeral no aplica a esta PC. 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

Este numeral no es aplicable ya que, para poder autenticar la identidad de una persona natural, este debe comparecer personalmente a la Oficina de Registro con su Documento Nacional de Identificación y, en caso de ser extranjero, Carnet de Residencia o Pasaporte Vigente.

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 Natural 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. ¿QUIÉN PUEDE REALIZAR UNA SOLICITUD?

La solicitud de Certificado de Persona Natural es efectuada por la persona natural, en posesión de su Documento Nacional de Identificación, Carnet de Residencia, o pasaporte vigente, que vaya a ser titular del certificado.

4.1.2. PROCESO DE ENROLAMIENTO Y RESPONSABILIDADES DE LOS SOLICITANTES

La persona natural que será el titular del certificado debe de solicitar cita a través de los medios que disponga la Administración Tributaria.

El día de la cita, el Solicitante se presenta a la Oficina de Registro seleccionada en dicha aplicación, en la que debe de portar el Documento Nacional de Identificación, Carnet de Residente o Pasaporte. Una vez verificada la documentación se procede a realizar el ingreso de los datos personales del solicitante en el sistema del PKI-SAR, así como la emisión del certificado.

Es responsabilidad del solicitante del certificado garantizar la completitud y veracidad de toda la información aportada para obtener sus Certificados de Persona Natural sin menos cabo en las comprobaciones realizadas por la Oficina de Registro.

4.2. GESTIÓN DE LAS SOLICITUDES DE CERTIFICADOS

4.2.1. FUNCIONES DE IDENTIFICACIÓN Y AUTENTICACIÓN

Para los certificados de persona natural, el solicitante aporta los datos que se le requieran, acreditan su Documento Nacional de Identificación o su Pasaporte. 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 los certificados de persona natural, una vez confirmadas la identidad del solicitante por el personal asignado a la Oficina de Registro, ésta procede a validar los datos y a enviar el certificado por medio de correo electrónico.

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

- Documento de identificación no es válido.
- Si el solicitante no tiene la acreditación suficiente (Carta Poder, entre otros).
- Si la información concerniente a identificación y autenticación de toda la información requerida en cada PC no está completa.

4.2.3. PLAZO PARA LA GESTIÓN DE LAS SOLICITUDES

Las PKI-SAR no se hacen responsables por el retraso que pueda surgir entre la solicitud del certificado y la entrega de este. En cualquier caso, el plazo para la tramitación de las solicitudes de certificados está condicionada a la capacidad operativa en las Oficinas de Registro.

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 en base a la solicitud, se realizan las notificaciones que se describen el apartado 4.3.2 Notificación al Solicitante de la Emisión por la AC del certificado.

La vigencia de los certificados inicia al momento de emisión de estos. El periodo 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 natural, la PKI-SAR informa por medio de correo electrónico al solicitante 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 natural, el solicitante acepta las condiciones de uso y expresa su voluntad de obtener el certificado, como requisitos necesarios para la generación del mismo.

4.4.2. PUBLICACIÓN DEL CERTIFICADO POR PARTE DE LA AC

No estipulado.

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 Natural son certificados de uso intransferible que acreditan la identidad de su titular.

4.5.1. USO DE LA CLAVE PRIVADA Y DEL CERTIFICADO POR EL SUSCRIPTOR

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 que haya expirado, lo que ocurra primero, el Suscriptor no puede usar la clave privada.

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

Los terceros deben confiar únicamente en los certificados para la realización de funciones que requieran acreditar la identidad del titular como persona natural y 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 de 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 natural; por loor 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

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 Natural, se debe de emitir siempre una nueva, siguiendo el mismo proceso que el descrito para la emisión de un certificado nuevo.

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

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 al Certificado de persona natural expedido. Por tanto, cualquier necesidad de modificación conlleva a la expedición de un nuevo

certificado. Consecuentemente, el resto de los incisos siguientes 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

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.

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 o un tercero en su nombre y representación, debidamente facultado, justificando el motivo de la revocación.
- Por muerte del Suscriptor.
- Compromiso de la clave privada del titular.
- 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.
- 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 tiene 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 natural solamente puede ser solicitado por:

- La autoridad judicial O de una entidad administrativa competente.
- El Suscriptor o un tercero en su nombre y representación.

La PKI-SAR puede revocar de oficio los certificados de persona natural 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 solicitud de revocación de Certificado de persona natural solamente puede ser solicitada por autoridad judicial O de una entidad administrativa competente, el titular o un tercero en su nombre o representación.

Una vez que la PKI-SAR ha procedido a la revocación del certificado de persona natural, 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. PERIODO EN QUE DEBE PROCESAR LAS SOLICITUDES DE REVOCACIÓN

No existe periodo 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, 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 laborales 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

Como establece la DPC de la PKI-SAR, en el numeral 4.9.6 denominado Requisitos de Verificación de las Revocaciones por los Terceros que Confían.

4.9.7. FRECUENCIA DE EMISIÓN DE CRL

Este apartado se detalla en la DPC de la PKI-SAR, en el numeral 4.9.7 denominando 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 apartado se detalla en la DPC de la PKI-SAR, en el numeral 4.9.8 denominando 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 apartado 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 aparatado se detalla en 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 apartado se detalla en la DPC de la PKI-SAR, en el numeral 4.9.12 denominando Causas para la Suspensión, de tal forma remitirse a lo ahí establecido.

4.9.13. QUIÉN PUEDE SOLICITAR LA SUSPENSIÓN

La solicitud puede presentarla la autoridad judicial, el titular del certificado o un tercero en su representación.

4.9.14. PROCEDIMIENTO PARA LA SOLICITUD DE SUSPENSIÓN

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

4.9.15. LÍMITES DEL PERIODO DE SUSPENSIÓN

Este apartado se detalla en la DPC de la PKI-SAR, en el numeral 4.9.15 denominado Límites del Período 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 apartado 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 aparatado 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 apartado se detalla en la DPC de la PKI-SAR, 4.10.3 denominado Características Adicionales, de tal forma remitirse a lo ahí establecido.

4.11. FINALIZACIÓN DE LA VALIDEZ DE UN CERTIFICADO

Este apartado 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 natural.

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 apartado 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 apartado 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 apartado 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 apartado 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 apartado 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 apartado 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 apartado 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 aparatado 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. OLES DE PKI-SAR

Este apartado 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 apartado 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 apartado 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 apartado 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 apartado 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 apartado se detalla en la DPC de la PKI-SAR, en el numeral 5.3.3 denominado Requerimientos de Formación, de tal forma remitirse a lo ahí establecido

5.3.4. REQUERIMIENTOS Y FRECUENCIA DE REENTRENAMIENTO

Este apartado se detalla en 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 apartado 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 apartado 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 apartado 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 apartado 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 apartado 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 aparatado 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 apartado se detalla en la DPC de la PKI-SAR, en el numeral 5.4.3 denominando 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 aparatado se detalla en DPC de la PKI-SAR, en el numeral 5.4.4 denominado Protección de los Registros de Auditoría.

5.4.5. PROCEDIMIENTOS DE RESPALDO DE LOS REGISTROS DE AUDITORIA

Este apartado 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 apartado 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

Este apartado se detalla e 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 apartado 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 apartado 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 apartado se detalla como establece 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 apartado 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 apartado 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 apartado 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

Este apartado se detalla en 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 apartado 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 apartado 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

Este apartado se detalla en 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 apartado 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 apartado 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 aparatado 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

Existen dos tipos de llaves: pública y privada. En relación con la generación de las claves del Suscriptor, es importante mencionar que la PKI-SAR no genera ni almacena las claves privadas asociadas a los certificados expedidos bajo la presente PC debido a que son generadas bajo el exclusivo control del Suscriptor.

6.1.2. ENTREGA DE LA LLAVE PRIVADA AL SUSCRIPTOR

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 natural son generada bajo el control exclusivo del Suscriptor 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 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 AC de PKI-SAR está a disposición de los terceros que confían en el Repositorio de PKI-SAR (ver apartado 2.1. Repositorios).

6.1.5. TAMAÑO DE LAS CLAVES

El tamaño de las claves de los certificados de persona natural 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 natural 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 natural 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 natural 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 apartado 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 natural no se encuentran bajo control multipersona. El control de dicha clave privada recae enteramente sobre el Suscriptor.

6.2.3. RESGUARDO DE LA CLAVE PRIVADA

La custodia de las claves privadas de los certificados de persona natural la realizan los Suscriptores 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 natural para garantizar el no repudio.

6.2.5. ARCHIVO DE LA CLAVE PRIVADA

Las claves privadas de firma de persona natural 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 natural para garantizar el no repudio.

6.2.7. ALMACENAMIENTO DE LA CLAVE PRIVADA EN UN MÓDULO CRIPTOGRÁFICO

Las claves privadas de firma de persona natural 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 titular de la misma mediante el uso de su contraseña de firma (únicamente conocido por él o ella).

6.2.9. MÉTODO DE DESACTIVACIÓN DE LA CLAVE PRIVADA

La desactivación de la clave privada de persona natural se realiza mediante solicitud autoridad judicial, el titular del certificado electrónico o un tercero en su nombre. 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 periodo de uso. La PKI-SAR dispone de un método de destrucción o almacenamiento 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 apartado 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 periodo de validez de los certificados de persona natural es no mayor a 3 años desde el momento de emisión de este.

6.4. DATOS DE ACTIVACIÓN

6.4.1. INSTALACIÓN Y GENERACIÓN DE LOS DATOS DE ACTIVACIÓN

Este apartado 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 apartado se detalla en la DPC de la PKI-SAR, en el numeral 6.4.2 denominado Protección para Datos de Activación, de tal forma remitirse a lo ahí establecido.

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 apartado 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 apartado 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 apartado 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 apartado 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 apartado 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 apartado 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 apartado 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 apartado 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 apartado 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 3.

7.1.2. EXTENSIONES DEL CERTIFICADO

A continuación, se detalla el contenido del certificado de firma electrónica avanzada de persona natural:

Contenido del certificado de firma electrónica avanzada de persona natural				
Nombre	**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	-

Contenido del certificado de firma electrónica avanzada de persona natural				
Nombre	**Atributo**	**Valor**	**Obligatorio**	**Crítica**
Validity	Not After	<fecha emisión>	Si	-
	Not Before	<fecha expiración>	Si	-
Subject	C	HN	Si	-
	O	<Nombre de la persona natural>	Si	-
	OU	FIRMA ELECTRONICA	Si	-
	CN	CN=[F] NOMBRE <apellidos nombre del representante> – DNI <documento nacional de identificación/pasaporte>	Si	-
Subject Public Key Info	Algorithm	RSA	Si	-

A continuación, se detalla el contenido de las extensiones más significativas de los certificados de persona natural:

Extensión del certificado de firma electrónica avanzada de persona natural				
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

Extensión del certificado de firma electrónica avanzada de persona natural				
Nombre	**Atributo**	**Valor**	**Obligatorio**	**Crítica**
Certificate Policies	policyIdentifier (OID)	1.3.6.1.4.1.52089.2.2	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	DistributionPoint Name (URI)	http://pki.sar.gob.hn/crlsar/crl.crl	Si	
Authority Information Access	cAIssuers (URI)	http://pki.sar.gob.hn/crlsar/casub.crt	Si	
	OCSP (URI)	http://ocsp2.sar.gob.hn/CryptosecOpenKey/va_service		

7.1.3. IDENTIFICADOR DE OBJETO (OID) DE LOS ALGORITMOS

El 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 Natural 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 PolicyConstrains del Certificado Raíz de la AC no es utilizado.

7.1.8. SINTAXIS Y SEMÁNTICA DE LOS "POLICYQUALIFIER"

La extensión CertificatePolicies contiene los siguientes PolicyQualifiers:

- 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 incluirá 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 "CertificatePolicy" incluye el campo OID de la política, que la 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 apartado se detalla en DPC de la PKI-SAR, en el numeral 7.3.2 denominado 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 apartado 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 apartado se detalla en la DPC de la PKI-SAR, en el numeral 8.2 denominando Identificación/Cualificación del Auditor, de tal forma remitirse a lo ahí establecido.

8.3. RELACIÓN ENTRE EL AUDITOR Y LA AUTORIDAD AUDITADA

Este apartado 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 apartado 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 apartado 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 apartado 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

La tarifa de emisión y renovación de cada Certificado de Firma Electrónica Avanzada de Persona Natural 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 aparado 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 apartado 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 apartado se detalla en la DPC de la PKI-SAR, en el numeral 9.3 denominado Cconfidencialidad de la Información, de tal forma remitirse a lo ahí establecido.

9.3.1. ALCANCE DE LA INFORMACIÓN CONFIDENCIAL

Este apartado 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 apartado 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

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

9.5. DERECHOS DE PROPIEDAD INTELECTUAL

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

9.6. OBLIGACIONES Y GARANTÍAS

9.6.1. OBLIGACIONES DE LA AC

Este apartado 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 apartado 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 DE LOS CERTIFICADOS

Este apartado se detalla en la DPC de la PKI-SAR, en el numeral 9.6.3 denominado Obligaciones de los Suscriptores 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 apartado 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.

9.7. EXENCIÓN DE RESPONSABILIDADES

Este apartado 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.

9.8. LIMITACIONES DE LAS RESPONSABILIDADES

Este apartado 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.

9.9. INDEMNIZACIONES

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

9.9.1. INDEMNIZACIONES DE LA CA

No estipulado.

9.9.2. INDEMNIZACIONES DE LOS SUSCRIPTORES

No estipulado.

9.9.3. INDEMNIZACIONES DE LAS PARTES QUE CONFÍAN

No estipulado.

9.10. PERÍODO DE VALIDEZ DE ESTE DOCUMENTO

9.10.1. PERIODO

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

9.10.2. TERMINACIÓN DE LA DPC

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

9.10.3. 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.

9.11. NOTIFICACIONES INDIVIDUALES Y COMUNICACIONES CON LOS PARTICIPANTES

Este apartado se detalla en 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.

9.12. MODIFICACIONES DE ESTE DOCUMENTO

9.12.1. PROCEDIMIENTO PARA LAS MODIFICACIONES

Este apartado 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.

9.12.2. PERIODO Y MECANISMO DE NOTIFICACIÓN

Este apartado se detalla en la DPC de la PKI-SAR, en el numeral 9.12.2 denomina Periodo y Mecanismo de Notificación, de tal forma remitirse a lo ahí establecido

9.12.3. CIRCUNSTANCIAS EN EL QUE EL OID DEBE SER CAMBIADO

Este apartado 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.

9.13. RESOLUCIÓN DE CONFLICTOS

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

9.14. NORMATIVA APLICABLE

Este apartado 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.

9.15. CUMPLIMIENTO DE LA LEGISLACIÓN APLICABLE

Este apartado 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.

9.16. ESTIPULACIONES MISCELÁNEAS

9.16.1. 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.

9.16.2. RESOLUCIÓN DE CONFLICTOS EN LA VÍA JUDICIAL

Este apartado 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.

9.17. OTRAS ESTIPULACIONES

No se consideran otras estipulaciones.