POLÍTICA

DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN DE INFRAESTRUCTURA DE CLAVE PÚBLICA DEL SERVICIO DE ADMINISTRACIÓN DE RENTAS DE LA REPUBLICA DE HONDURAS

POL-GIF-GGI-001-V1

SAR

SERVICIO DE ADMINISTRACIÓN DE RENTAS

SECRETARÍA GENERAL

Diciembre 2021

FECHA VIGENCIA: Diciembre - 2021	CÓDIGO: POL-GIF-GGI-001-V1	VERSIÓN 1.0	Nº PÁGINAS 74

POLÍTICA
DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN DE INFRAESTRUCTURA DE CLAVE PÚBLICA DEL SERVICIO DE ADMINISTRACIÓN DE RENTAS DE LA REPUBLICA DE HONDURAS

RUBRO	CARGO	FIRMA
APROBADO POR:	Abg. Miriam Estela Guzmán Bonilla **Directora Ejecutiva**	
	Abg. Angela María Madrid **Sub Directora Ejecutiva**	
REVISADO POR:	Abg. Carmen Alejandra Suarez Pacheco **Secretaria General**	
	Abg. Cristian Erazo **Director Nacional Jurídico**	
	Abg. Fátima Isabel Estrada Saravia **Experto de la Dirección Nacional Jurídica**	
	Ing. Diana Orestila Cárcamo Rodríguez **Directora Nacional de Tecnología**	
	Ing. Nathaly Nuñez **Jefe Gestión de Procesos**	
ELABORADO POR:	Ing. Osman René Moreno Ramos **Experto Dirección Nacional De Tecnología**	
	Abg. Carlos Antonio García Garcia **Especialista de Secretaria General**	
	Ing. Francisco Rafael Domínguez O´Hara **Analista De Gestión 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. CONTROL DEL DOCUMENTO

Versión	Motivo	Fecha de vigencia	Documentos que elimina
1.0	Creación	Diciembre-2021	N/A

2. OBJETIVO ESTRATÉGICO VINCULADO AL DOCUMENTO

OBJETIVO ESTRATÉGICO
Objetivo estratégico 1: Incrementar la recaudación de manera sostenida mediante la promoción del cumplimiento voluntario de las obligaciones tributarias.
Objetivo Estratégico 2: Reducir los costos del cumplimiento a través de la estandarización de procesos y el uso de tecnologías de la información y comunicaciones.
Objetivo Estratégico 3: Combatir la evasión fiscal a través del control de las obligaciones tributarias y el cobro de los tributos internos.

3. DOCUMENTO RELACIONADO

Nombre del Documento Relacionado	Código o número de acuerdo o del Documento Relacionado
Estatuto Orgánico	Acuerdo Número SAR-109-2019

4. ÁREA O DEPARTAMENTO RELACIONADO PARA ESTE DOCUMENTO

Dirección	Departamento	Unidad o Coordinación
Secretaria General	N/A	Archivo
		Acceso a la Información Pública
		Recepción y Notificación
Dirección de Talento Humano	Departamento de Planificación y Desarrollo del Talento Humano	N/A
	Departamento de Gestión del Talento Humano	N/A
Dirección Nacional de Tecnología	Departamento de Gestión Aplicaciones	N/A
	Departamento de Infraestructura y Redes	N/A
Dirección Nacional Juridico	Departamento de Asesoria y Procuración Legal	N/A

5. 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

6. OBJETIVO

El presente documento recoge las Políticas de certificación, las cuales regirán el funcionamiento y operaciones de la Infraestructura de Clave Pública de Servicio de Administración de Rentas de Honduras (PKI).

7. ALCANCE

La totalidad de los certificados emitidos por la PKI de Servicio de Administración de Rentas de Honduras, cumplen con lo estipulado en la versión 3 del estándar X.509, de esta manera se hace posible la adición de extensiones para la certificación de atributos.

8. EXCLUSIONES

Este documento ha sido diseñado basado en las recomendaciones de la RFC 7382, con la finalidad de hacer este documento de fácil comprensión para el lector, existirán secciones las cuales determinaremos como "No Estipulado", dichas secciones del documento no tienen inherencia en nuestro marco de cumplimiento.

9. MARCO LEGAL

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
Resolución No. 002-2017	2017	Autorización al SAR como Autoridad Certificadora o Prestadora de Servicios de Certificación PSC
Acuerdo SAR 374-2018	2018	Creación de Comité de Firma Electrónica
Demás disposiciones legales aplicables		

10. MARCO TÉCNICO

Documentos de Referencia	Fecha de vigencia
Versión 3 del estándar X.509	2008
Recomendaciones del RFC 7382	2015

11. NARRATIVA

11.1 NOMBRE DEL DOCUMENTO E IDENTIFICACIÓN DE LA DPC

El nombre de este documento es "Declaración de Prácticas de Certificación, para la Infraestructura de Clave Pública del Servicio de Administración de Rentas de la República de Honduras", el presente se encuentra en su **versión 1.0** y será vigente a partir de su fecha de aprobación y publicación hasta el momento en que sea publicada una nueva versión del mismo; el URL para acceder públicamente a este documento se encuentra en la siguiente dirección https://www.sar.gob.hn/firmaelectronica/ El OID correspondiente a este documento es el siguiente: 2.16.340.1.1.2.1

11.2 PARTICIPANTES DE LA PKI

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

1. Autoridades de Certificación (AC)
2. Autoridades de Registro (AR)
3. Autoridades de Validación (AV)
4. Solicitantes y Suscriptores de certificados
5. Terceros que confían en los certificados de la PKI del Servicio de Administración de Rentas
6. Autoridad Administrativa Competente (AAC)
7. Prestador de Servicios de Certificación (PSC)

11.2.1 AUTORIDADES DE CERTIFICACIÓN (AC)

Comprende el grupo de individuos, procedimientos, políticas y sistemas informáticos, los cuales tienen como tarea principal la emisión de certificados electrónicos y la asignación de estos a sus Suscriptores correspondientes. 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.

11.2.1.1 AUTORIDAD CERTIFICADORA RAÍZ DE HONDURAS

La SAR-PKI será la designada para realizar la emisión de los certificados, los cuales son objeto de la presente DPC regida bajo el Certificado Raíz. El Certificado raíz consiste en un certificado auto firmado en con el cual se da inicio a la cadena de confianza.

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

En la siguiente tabla se detallan los datos con más relevancia de la autoridad certificadora de Servicio de Administración de Rentas.

Nombre distintivo	**CN=AUTORIDAD CERTIFICADORA DEL SAR, O=SERVICIO DE ADMINISTRACION DE RENTAS OU=SECRETARÍA GENERAL, C=HN, L= TEGUCIGALPA, ST= FRANCISCO MORAZAN**
Número de serie	
Nombre distintivo del emisor	**CN=AUTORIDAD CERTIFICADORA DEL SAR, O=SERVICIO DE ADMINISTRACION DE RENTAS OU=SECRETARÍA GENERAL, C=HN, L= TEGUCIGALPA, ST= FRACISCO MORAZAN**
Fecha de emisión	**AAAA-MM-DD HH:MM:SS**
Fecha de expiración	**AAAA-MM-DD HH:MM:SS**
Longitud de clave RSA	**4096**
Huella digital (SHA-1)	
URL de publicación del certificado	**https://www.sar.gob.hn/firmaelectronica/**
URL de Publicación de ARL	**http://pki.sar.gob.hn/crls/arl.crl**

11.2.1.2 AUTORIDAD CERTIFICADORA SUBORDINADA DEL SAR

La PKI del Servicio de Administración de Rentas implementará una AC subordinada. Dicha AC es la siguiente en jerarquía a la AC Raíz, por tanto, la AC Subordinada será la encargada de la emisión de todos los certificados para persona natural, persona jurídica o funcionarios Públicos

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

Nombre distintivo	CN= AC SUBORDINADA DEL SAR, O=SERVICIO DE ADMINISTRACION DE RENTAS OU=SECRETARÍA GENERAL, C=HN, L= TEGUCIGALPA, ST= FRANCISCO MORAZAN
Número de serie	
Nombre distintivo del emisor	CN=AUTORIDAD CERTIFICADORA DEL SAR, O=SERVICIO DE ADMINISTRACION DE RENTAS OU=SECRETARÍA GENERAL, C=HN, L= TEGUCIGALPA, ST= FRACISCO MORAZAN
Fecha de emisión	AAAA-MM-DD HH:MM:SS
Fecha de expiración	AAAA-MM-DD HH:MM:SS
Longitud de clave RSA	4096
Huella digital (SHA-1)	
URL de publicación del certificado	https://sar.gob.hn/firmaelectronica/
URL de publicación de CRL	http://pki.sar.gob.hn/crls/crl.crl
Tipos de Certificados Emitidos	Firma de Funcionario Público

11.2.2 AUTORIDAD DE REGISTRO (AR)

Es el órgano designado por la Autoridad Administrativa Competente (AAC) para realizar recepción de solicitudes, validación de información y aprobación de emisión de los Certificados Electrónicos.

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 las circunstancias personales de la persona que constará 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.

11.2.3 AUTORIDADES 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 el estándar RFC2560.

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 CRL.

11.2.4 SOLICITANTES Y SUSCRIPTORES DE CERTIFICADOS

Los solicitantes y suscriptores de certificados son definidos por la DPC de la SAR-PKI. Dentro del contexto de esta PC, los suscriptores y solicitantes de "Certificado de Firma Electrónica" es cualquier persona natural que posea una tarjeta de identidad de Honduras o un extranjero residente en Honduras con pasaporte vigente, Personas Juridicas debidamente registradas en el territorio nacional y Funcionarios Públicos con la documentación que garantice su pertenencia en el Estado

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

Los terceros que confían son comprendidos por las entidades o personas que confían en los certificados emitidos por la AC de la SAR-PKI con la finalidad de asegurar la identidad de un suscriptor como persona natural.

11.2.6 AUTORIDAD ADMINISTRATIVA COMPETENTE (AAC)

La Dirección General de Propiedad Intelectual (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; 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.

11.2.7 PRESTADOR DE SERVICIOS DE CERTIFICACIÓN (PSC)

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

- Emitir certificados en relación con las Firmas Electrónicas certificadas de Funcionario Público.
- 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.

Podrán actuar como Autoridades Certificadoras o Prestadores de Servicios de Certificación (PSC), 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); y conforme las condiciones siguientes:

- Contar con la capacidad económica y financiera suficiente para prestar los servicios autorizados como autoridad certificadora, así como con el recurso humano y la de ontología 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 confien en éste.

Para verificar que las Autoridades Certificadoras o Prestadores de Servicios de Certificación (PSC) cumplan con los requerimientos antes establecidos y para determinar el grado de fiabilidad de dichos prestadores se tomarán los factores 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 deberá ser competente para las funciones que realiza, incluyendo 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).

11.3 USO DE LOS CERTIFICADOS

El uso adecuado del certificado se determina por medio de las Políticas de Certificación correspondientes a cada tipo de Certificado. El objetivo de esta DPC no es el de determinar dichos usos.

11.3.1 PROHIBICIONES DE USO DE LOS CERTIFICADOS.

Los Certificados deben ser empleados para los usos detallados explícitamente a la DPC correspondiente y se prohíbe su uso para cualquier actividad o fines no contemplados en dicha DPC.

11.4 ADMINISTRACIÓN DE LAS POLÍTICAS

11.4.1 ORGANIZACIÓN RESPONSABLE DE LA DPC

Los términos y redacción de la presente DPC de SAR-PKI, serán establecidos por Servicio de Administración de Rentas a través de su Secretaria General y de la Dirección Nacional de Tecnología; estas entidades serán responsables también de realizar revisiones periódicas a las mismas, de manera que se mantengan actualizadas. La AAC Autoridad Administrativa Competente, será la responsable de establecer el plazo de las revisiones antes mencionadas, sin embargo, en ningún caso este período podrá ser mayor a 12 meses.

11.4.2 DATOS DE CONTACTO

Nombre de Entidad: Servicio de Administración de Rentas

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) 2235-2150 EXT. 1007

11.4.3 PERSONA O COLECTIVO RESPONSABLE POR MODIFICACIONES A LA DPC

La responsabilidad de las aprobaciones y modificaciones correspondientes de la DPC corresponde de manera exclusiva al Comité Institucional de Firma Electrónica, de acuerdo con las facultades otorgadas a dicho Comité por parte de Servicio de Administración de Rentas.

Todas las modificaciones realizadas a la DPC deberán ser publicadas en el sitio web de Servicio de Administración de Rentas, en la dirección http://ocsp.sar.gob.hn/CryptosecOpenKey/va_service. En caso de haber 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 dará derecho al Suscriptor de recibir compensación por este motivo.

11.5 REPOSITORIOS Y PUBLICACIÓN DE INFORMACIÓN

11.5.1 REPOSITORIOS

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

Servicio de validación en línea que implementa el protocolo OCSP	**http://ocsp.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/crls/arl.crl
Certificado de CA Subordinada	https://sar.gob.hn/firmaelectronica/
CRL de CA Subordinada	http:// pki.sar.gob.hn/crls/crl.crl

11.5.2 PUBLICACIÓN DE INFORMACIÓN DE CERTIFICACIÓN

Como parte de las obligaciones y responsabilidades de las AC pertenecientes a la Jerarquía de confianza de la SAR-PKI, deben realizar la publicación de sus prácticas, certificados y estatus actual de los mismos.

Esta DPC es de carácter público y se encuentra publicado en el sitio web de SAR-PKI, al que se hace mención en el numeral 11.5.1. Repositorios.

Las Políticas de Certificación (PC), son de carácter público y se encuentran publicadas en el sitio web de SAR-PKI, al que se hace mención en el numeral 11.5.1. Repositorios.

Las Listas de Revocación de Certificados (CRL), son de carácter público y se encuentran publicadas en el servidor web de SAR-PKI, al que se hace mención en el numeral 11.5.1. Repositorios.

El estado de los certificados emitidos podrá ser consultado haciendo uso del servicio de validación en línea correspondiente al protocolo OCSP o en su defecto haciendo uso de las CRL.

11.5.3 TIEMPOS Y FRECUENCIA DE PUBLICACIÓN

La Declaración de Políticas de Certificación (DPC) serán publicadas al momento de creación y sus modificaciones serán publicadas consecuentemente al momento de su aprobación. Dicha documentación será publicada en el sitio web al que se hace mención en el numeral 11.5.1. Repositorios.

La AC agregará los certificados que hayan sido revocados a la CRL correspondiente, la ventana de tiempo deberá ser acorde al punto 11.7.9.7. Frecuencia de emisión de CRL.

11.5.4 CONTROLES DE ACCESO A LOS REPOSITORIOS

El acceso a la información de certificación, entiéndase por esta las DPC, es de carácter público, sin embargo, el único ente autorizado para realizar modificaciones, sustituciones o eliminación de información del sitio web y repositorios es SAR-PKI. Por tal motivo SAR-PKI será responsable de establecer los controles necesarios para que personas no autorizadas no puedan manipular la información que reposa en dichos repositorios.

11.6 IDENTIFICACIÓN Y AUTENTICACIÓN

11.6.1 NOMBRES

11.6.1.1 TIPOS DE NOMBRES

La totalidad de los Suscriptores de certificados requieren de un Nombre Distintivo (Distinguished Name) el cual debe cumplir con el estándar X.500

El proceso para realizar la asignación de los Nombres Distintivos (DN) para cada uno de los suscriptores en base al tipo de certificado, es definido por la Política de certificación correspondiente a cada tipo de certificado. Las PC

antes mencionadas deben ser acordes a las directrices descritas en esta DPC.

11.6.1.2 NECESIDAD DE QUE LOS NOMBRES SEAN SIGNIFICATIVOS

Se recomienda que los nombres significados de los Suscriptores de los certificados sean significativos para todos los casos.

La necesidad de dar significado a los Nombres Distintivos está estipulada por la política de certificación correspondiente al certificado en cada caso.

11.6.1.3 REGLA PARA INTERPRETAR VARIOS FORMATOS DE NOMBRES

La SAR-PKI hará 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.

11.6.1.4 UNICIDAD DE LOS NOMBRES

La agrupación del Nombre Distintivo (DN) más el contenido de la extensión Policy Indentifier debe ser único y no confuso.

Con el propósito de garantizar la unicidad para cada tipo de certificado, se han establecido procesos listados en la Política de Certificación correspondiente.

11.6.1.5 RECONOCIMIENTO, AUTENTICACIÓN Y PAPEL DE LAS MARCAS REGISTRADAS

Este numeral no aplica a esta DPC, ya que la SAR-PKI, no asume compromiso de marcas comerciales al momento de la emisión de los certificados electrónicos expedidos bajo la PC correspondiente. La SAR-PKI se reserva el derecho de rechazar solicitudes que presenten conflictos de nombres de marcas comerciales.

11.6.2 VALIDACIÓN INICIAL DE IDENTIDAD

11.6.2.1 CRITERIOS PARA INTEROPERABILIDAD

De acuerdo con lo establecido en el Reglamento de Ley Sobre Firmas Electrónicas, Acuerdo Ejecutivo Número 41-2014, publicado en el Diario Oficial La Gaceta el 21 de mayo de 2015, establece que toda Firma Electrónica creada o utilizada fuera de la República de Honduras producirá los mismos efectos jurídicos que una firma creada o utilizada en Honduras, si presenta un grado de fiabilidad equivalente.

Los Certificados de Firmas Electrónicas emitidos por Autoridades o Entidades de Certificación extranjeras, producirán los mismos efectos jurídicos que un certificado expedido por Autoridades Certificadoras Nacionales, siempre y cuando tales certificados presenten un grado de fiabilidad en cuanto a la regularidad de los detalles de este, así como su validez y vigencia.

A efectos de determinar si un Certificado de Firmas Electrónicas o una Firma Electrónica presentan un grado de fiabilidad sustancialmente equivalente para los fines de los párrafos anteriores, se tomarán en consideración las normas internacionales reconocidas y cualquier otro factor pertinente; ya que lo que se pretende es contrastar su fiabilidad con los requisitos establecidos en el Articulo 8 de la "Ley Sobre Firmas Electrónicas" y su Reglamento considerando que el grado de fiabilidad de un certificado extranjero debe ser equivalente al grado de fiabilidad de un certificado nacional.

11.6.3 IDENTIFICACIÓN Y AUTENTICACIÓN PARA SOLICITUDES DE RENOVACIÓN

El procedimiento dispuesto para realizar la autenticación e identificación individual se encuentra definido por la Política de Certificación correspondiente.

11.6.4 IDENTIFICACIÓN Y AUTENTICACIÓN PARA SOLICITUDES DE REVOCACIÓN

El procedimiento dispuesto para realizar la autenticación e identificación individual se encuentra definido por la Política de Certificación correspondiente.

11.7 REQUISITOS OPERACIONALES PARA EL CICLO DE VIDA DE LOS CERTIFICADOS

11.7.1 SOLICITUD DE CERTIFICADOS

El procedimiento establecido para la emisión de certificados de firma electrónica está establecido por la Política de Certificación correspondiente.

11.7.1.1 QUIEN PUEDE REALIZAR UNA SOLICITUD

Las políticas de certificación correspondientes definen quién tiene la potestad de realizar la solicitud de certificados, así como la información que debe ser proporcionada al momento de realizar la solicitud. Dicha PC deberá detallar los pasos que deben seguirse para completar este proceso.

11.7.1.2 PROCESO DE ENROLAMIENTO Y RESPONSABILIDADES DE LOS SOLICITANTES

Es potestad de cada Autoridad de registro de la SAR-PKI el discernir el tipo de certificado que se ajuste a las características del solicitante, esto siguiendo las disposiciones de la PC correspondiente a cada caso. La Autoridad de registro tiene la potestad de rechazar o aprobar la solicitud de certificación.

Los solicitantes serán responsables por la falsedad, error u omisión en la información suministrada al prestador de servicios de certificación y por el incumplimiento de sus obligaciones como suscriptor.

El Proceso de enrolamiento es descrito en la Política de Certificación correspondiente a cada caso.

11.7.2 GESTIÓN DE LAS SOLICITUDES DE CERTIFICADOS

11.7.2.1 FUNCIONES DE IDENTIFICACIÓN Y AUTENTICACIÓN

El proceso de Identificación individual se encuentra estipulado por la Política de Certificación correspondiente a cada tipo de certificado.

11.7.2.2 RECHAZO O ACEPTACIÓN DE SOLICITUDES DE CERTIFICADO

El certificado será emitido una vez la SAR-PKI haya realizado el proceso de verificación necesario para validar la solicitud de certificación. Dicho procedimiento será establecido en la política de certificación que corresponde a cada tipo de certificado.

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

- Documento de identificación no es válido; o
- El solicitante no tiene autorización para solicitar la emisión de certificado.
- Si la información concerniente a identificación y autenticación de toda la información requerida en cada política de certificación no puede ser completada; o
- La inexistencia de registro de datos en la Institución a la que el sujeto pertenece o los datos no son consistentes con la forma de solicitud de certificación;
- Y otras dependiendo de la particularidad de la documentación solicitada para cada tipo certificado, las que se estipularán en cada una de las políticas de certificación correspondientes.

11.7.2.3 PLAZO PARA LA GESTIÓN DE LAS SOLICITUDES

Las AC de la SAR-PKI no se harán responsables por retrasos que puedan surgir entre la solicitud del certificado y la entrega de este. Los plazos para la tramitación dependerán de las Políticas de certificación correspondientes.

11.7.3 EMISIÓN DE CERTIFICADOS

11.7.3.1 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 realizarán las notificaciones que se describen el apartado 11.7.3.2 del presente capitulo.

La vigencia de los certificados inicia al momento de emisión de estos. El periodo de validez o vigencia del certificado podrá 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.

Lo establecido en el presente numeral queda subordinado a lo establecido en las diferentes políticas de certificación correspondientes a cada certificado.

11.7.3.2 PROCESO DE NOTIFICACIÓN AL SOLICITANTE DE LA EMISIÓN POR LA AC DEL CERTIFICADO

Se procederá de manera que al momento aprobación de solicitud del certificado, el solicitante o suscriptor será notificado mediante la dirección de correo electrónico suministrada al momento de realizada la solicitud.

11.7.4 ACEPTACIÓN DEL CERTIFICADO POR EL ENTE FINAL

11.7.4.1 ACCIÓN QUE AFIRMA LA ACEPTACIÓN DEL CERTIFICADO

Salvo acuerdo entre las partes, se entiende que un suscriptor ha aceptado un certificado cuando la Autoridad Certificadora, a solicitud de éste o de una persona en nombre de éste, lo ha guardado técnica y adecuadamente.

11.7.4.2 PUBLICACIÓN DEL CERTIFICADO POR PARTE DE LA AC

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

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

En el momento que una de las AC del SAR-PKI emita un certificado en base a una solicitud generada a través de una AR, la AC enviará una copia de este a la RA que procesó la solicitud.

11.7.5 USO DEL PAR DE CLAVES Y CERTIFICADO

11.7.5.1 USO DE LA CLAVE PRIVADA Y DEL CERTIFICADO POR EL SUSCRIPTOR

Las responsabilidades y limitaciones asociadas a la utilización del par de claves y el certificado, serán definidas en los términos y condiciones correspondiente a cada caso. De cualquier forma, el Suscriptor, solo podrá emplear el certificado y la clave privada para los usos descritos en las políticas de certificación correspondientes y de conformidad con lo que establecen los campos de "Key Usage" y "Extended Key Usage" del certificado. El Suscriptor solo podrá utilizar el par de llaves y certificado una vez sean aceptadas las condiciones de uso, las cuales son establecidas en la DPC y PC.

Una vez haya sido revocado el certificado o haya expirado, lo que ocurra primero, el suscriptor no podrá de usar la clave privada.

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

Los terceros que confían deben únicamente confiar en los certificados para las acciones o procedimiento que se hayan establecido en la PC que aplique a cada caso y de conformidad con lo establecido en el campo "key Usage" y "extended key usage" del certificado en cuestión.

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 esta DPC y la PC que corresponda a cada caso.

De la misma forma son sujeto de cumplimiento de las condiciones de uso establecidas en los documentos antes mencionados.

11.7.6 RENOVACIÓN DE CERTIFICADOS - CAMBIO DE CLAVE AUSENTE

11.7.6.1 CIRCUNSTANCIAS PARA LA RENOVACIÓN DE CERTIFICADOS - CAMBIO DE CLAVE AUSENTE

La totalidad de las renovaciones de certificados llevadas a cabo bajo el ámbito de la presente DPC serán llevados a cabo con cambio de claves. Por lo tanto, los puntos referentes a la renovación de certificados sin cambios de clave (puntos 11.7.6.2 11.7.6.3 11.7.6.4 11.7.6.5 11.7.6.6), los cuales son establecidos en el RFC 3647, lo cual, por consecuencia a efectos de esta DPC, su no estipulación.

11.7.6.2 QUIÉN PUEDE SOLICITAR LA RENOVACIÓN DE LOS CERTIFICADOS - CAMBIO DE CLAVE AUSENTE

No estipulado

11.7.6.3 NOTIFICACIÓN DE LA EMISIÓN DE UN NUEVO CERTIFICADO AL SUSCRIPTOR

No Estipulado

11.7.6.4 FORMA DE ACEPTACIÓN DEL CERTIFICADO - CAMBIO DE CLAVE AUSENTE

No Estipulado

11.7.6.5 PUBLICACIÓN DEL CERTIFICADO - CAMBIO DE CLAVE AUSENTE

No Estipulado

11.7.6.6 NOTIFICACIÓN DE LA EMISIÓN DEL CERTIFICADO POR LA CA A OTRAS AUTORIDADES

No Estipulado

11.7.7 RENOVACIÓN DE CERTIFICADOS CON CAMBIO DE CLAVES

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

El procedimiento para la renovación de certificados corresponde a la Política de Certificación aplicada a cada caso.

Algunos de los motivos que harían necesaria la renovación de un certificado son:

- Expiración del periodo de vigencia.
- Cambio de datos contenidos en el certificado.
- Claves comprometidas o pérdida de confiabilidad de estas.
- Cambio en el formato.
- Pérdida del certificado.

La totalidad de las renovaciones de certificados de la SAR-PKI se realizarán con cambio de claves.

11.7.7.2 QUIÉN PUEDE PEDIR LA RENOVACIÓN DE LOS CERTIFICADOS

Las políticas de Certificación correspondientes a cada caso establecerán quien tiene la potestad de solicitar la renovación de un certificado.

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

La política de certificación correspondiente a cada caso establecerá los procesos de identificación y autenticación, sin embargo, en caso de conflicto prevalecerá lo establecido en este numeral.

En todos los casos, la renovación de un certificado está condicionada a:

- Que la solicitud de renovación sea realizada en debido tiempo y forma, de acuerdo con las instrucciones y normativa establecidas por la SAR-PKI para este propósito.
- Que la CA no haya sido notificada sobre la concurrencia de causa alguna de revocación o suspensión del certificado.
- La solicitud de renovación de los servicios de prestación sea estipulada para el mismo tipo de certificado emitido en primera instancia.

11.7.7.4 NOTIFICACIÓN DE LA EMISIÓN DE UN NUEVO CERTIFICADO AL SUSCRIPTOR

Las PC correspondientes a cada tipo de certificado establecerán el medio y forma de comunicación mediante el cual el solicitante será informado de la emisión de un certificado en su nombre.

11.7.7.5 MÉTODO DE ACEPTACIÓN DEL CERTIFICADO CON CAMBIO DE CLAVES

Las PC correspondientes a cada tipo de certificado establecerán la forma de aceptación.

11.7.7.6 PUBLICACIÓN DEL CERTIFICADO CON LAS NUEVAS CLAVES POR PARTE DE LA CA

Las PC correspondientes a cada tipo de certificado, establecerán si procede o no y el método de publicación del certificado.

11.7.7.7 NOTIFICACIÓN DE LA EMISIÓN DEL CERTIFICADO POR LA CA A OTRAS AUTORIDADES

En el momento en que la CA de la SAR-PKI, realice la emisión de un certificado de acuerdo con una solicitud de certificación tramitada mediante una RA, la CA realizará él envió de una copia de éste a la RA que remitió la solicitud.

11.7.8 MODIFICACIÓN DE CERTIFICADOS

11.7.8.1 CIRCUNSTANCIAS PARA LA MODIFICACIÓN DEL CERTIFICADO

La modificación de un certificado denota el proceso en el cual se emite uno nuevo debido a cambios en la información del certificado, no relacionados con su clave pública o expiración del periodo de vigencia.

Las modificaciones de los certificados pueden venir dadas por diferentes motivos tales como:

- Modificación de nombre.
- Modificación en las funciones dentro de la organización.
- Cualquier cambio que tenga como resultado algún cambio en el Nombre Distintivo.

La totalidad de las modificaciones de certificados realizadas en torno a esta DPC serán tratadas como una renovación de certificados, por lo tanto, deberán aplicarse los numerales anteriores al respecto.

11.7.8.2 QUIÉN PUEDE SOLICITAR LA MODIFICACIÓN DE LOS CERTIFICADOS

Este numeral no es aplicable, dado que la totalidad de las solicitudes de modificación de certificado serán procesadas como una renovación de

certificados. Por lo tanto, serán aplicados los numerales anteriores referentes a la renovación. Consecuentemente el resto de los puntos referentes a la modificación de certificados (puntos 11.7.8.3 11.7.8.4 11.7.8.5 11.7.8.6 11.7.8.7) establecidos por la RFC3647, lo que implica, a efectos de esta DPC, su no estipulación.

11.7.8.3 GESTIÓN DE LAS PETICIONES DE MODIFICACIÓN DE CERTIFICADOS

No estipulado.

11.7.8.4 NOTIFICACIÓN POR LA EMISIÓN DE UN CERTIFICADO MODIFICADO AL SUSCRIPTOR

No estipulado.

11.7.8.5 MÉTODO DE ACEPTACIÓN DEL CERTIFICADO MODIFICADO

No estipulado.

11.7.8.6 PUBLICACIÓN DEL CERTIFICADO MODIFICADO POR LA CA

No estipulado.

11.7.8.7 NOTIFICACIÓN DE LA MODIFICACIÓN DEL CERTIFICADO POR LA CA A OTRAS ENTIDADES

No estipulado.

11.7.9 REVOCACIÓN Y SUSPENSIÓN DE CERTIFICADOS

11.7.9.1 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). Al alcanzar la fecha de expiración de un certificado revocado, el mismo será removido de la CRL.

El suscriptor de una firma digital certificada podrá solicitar al SAR-PKI, la revocación de este. En todo caso, estará obligado a solicitar revocación en los eventos siguientes:

- Por perdida de la clave privada; y,
- Exposición de la clave privada y peligro de uso indebido.

Si el suscriptor no solicita la revocación del certificado en el evento de presentarse las anteriores situaciones, será responsable por las pérdidas o perjuicios en los cuales incurran terceros de buena fe, que confiaron en el contenido del certificado.

Sin exclusión o detrimento de lo dispuesto en la norma aplicable un certificado podrá ser revocado por:

- A petición del suscriptor o un tercero en su nombre y representación;
- Por muerte del suscriptor;
- Por liquidación del suscriptor en el caso de las personas jurídicas;
- Por la confirmación de que alguna información o hecho contenido en el certificado es falso;
- La clave privada de SAR-PKI o su sistema de seguridad ha sido comprometido de manera material que afecte la confiabilidad del certificado;
- Por el cese de actividades de SAR-PKI;
- Por orden judicial o de Autoridad Administrativa competente;
- Por declaración de insolvencia, siempre que, en el plazo fijado por ley, no se levante dicho estado; y,
- Cualquier otra causa lícita prevista en la declaración de prácticas de certificación.

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

11.7.9.2 QUIÉN PUEDE SOLICITAR LA REVOCACIÓN

La revocación puede ser solicitada de manera oficiosa por la SAR-PKI o cualquiera de las autoridades que la componen, en el caso de conocimiento o sospecha que la clave privada del Suscriptor haya sido comprometida o cualquier otro hecho mayor que requiriera ejecutar dicha acción.

Asimismo, los Suscriptores de certificados o sus responsables, en el caso de los certificados de componente, también podrán solicitar la revocación de sus certificados, debiendo hacerlo de acuerdo con las condiciones especificadas en el apartado 11.7.9.3.

La revocación también puede ser solicitada por el Suscriptor o sus responsables, acogiéndose a las condiciones descritas en el numeral 11.7.9.3 procedimiento de solicitud de revocación.

El procedimiento de identificación para la solicitud de revocación podrá ser el mismo utilizado para el registro inicial. Sin embargo, la política el procedimiento de autenticación solamente aceptará solicitudes firmadas electrónicamente por el Suscriptor del certificado, siempre y cuando el certificado utilizado sea diferente del certificado que se desea será revocado.

Las PC podrian definir politicas o procedimientos más estrictos.

11.7.9.3 PROCEDIMIENTO DE SOLICITUD DE REVOCACIÓN

La PC correspondiente a cada tipo de certificado definirá el procedimiento para la solicitud de revocación.

De forma general y sin perjuicio de lo definido en las PC se establece que:

- Se comunicará al Suscriptor del certificado la revocación de este mediante correo electrónico.
- Posterior a la revocación del certificado el Suscriptor deberá suspender el uso de la clave privada que se corresponda con dicho certificado.
- En el caso de certificados de persona natural, la revocación de un certificado de autenticación tendrá como consecuencia la revocación del resto de certificados asociados a un Suscriptor.

- La solicitud de revocación realizada o recibida con fecha posterior a la vigencia del certificado no será atendida.

La política de Certificación especificará la información necesaria para realizar la solicitud de revocación de un certificado.

11.7.9.4 PERIODO EN QUE UNA AUTORIDAD CERTIFICADORA DEBE PROCESAR LAS SOLICITUDES DE REVOCACIÓN

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

11.7.9.5 PLAZO EN EL QUE LA AC DEBE RESOLVER LA SOLICITUD DE REVOCACIÓN

Las Políticas de Certificación correspondientes a cada certificado, establecerán el tiempo máximo de resolución para las solicitudes de revocación, sin embargo, se establece como norma general que las mismas deben ser resueltas en menos de 24 horas.

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

Se debe realizar la verificación de las revocaciones mediante el protocolo OCSP o en su defecto mediante las CRL, esta disposición es de carácter obligatorio para cada uso de certificados por los Terceros que confían.

Se debe recurrir a la autoridad de validación mediante el protocolo OCSP para verificar las revocaciones, en caso de no disponibilidad de este servicio, deberán consultar las CRL dispuestas de manera pública para este fin, salvo que la PC establezca lo contrario.

En el caso de que la PC acepte otras formas para la divulgación de información de revocación, los requisitos para dicha comprobación serán especificados en dicha PC.

11.7.9.7 FRECUENCIA DE EMISIÓN DE CRL

Los métodos de verificación serán mediante el protocolo OCSP y mediante las CRL. La SAR-PKI publicará una nueva CRL en su repositorio correspondiente al momento en que se realice cualquier revocación. No obstante, la SAR-PKI publicará una nueva CRL en el repositorio correspondiente en espacios de tiempo no mayores a 72 horas para las AC subordinadas, para el caso de la ARL de la AC Raíz, deberá realizarse la publicación de esta al instante en que se efectúe la revocación del Certificado de la AC Subordinada el intervalo de publicación de una nueva ARL no debe ser superior a un (1) año en caso en que haya o no revocaciones.

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

Las PC correspondientes a cada tipo de certificado establecerán el periodo de tiempo máximo aceptable entre la generación y publicación de las CRL en su repositorio. Sin embargo, para el caso de la LRA de la AC Raíz, deberá realizarse la publicación de esta al instante en que se efectúe la revocación del Certificado de la AC Subordinada.

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

La SAR-PKI pone a disposición una Autoridad de Validación que permite verificar el estado de los certificados mediante el protocolo OCSP.

11.7.9.10 REQUISITOS DE COMPROBACIÓN EN LÍNEA DE REVOCACIÓN

Con el fin de ser capaz de interactuar con la autoridad de validación, el tercero que confía debe disponer de un componente de software que le permita operar con el protocolo OCSP para obtener la información de estado del certificado.

11.7.9.11 OTRAS FORMAS DE DIVULGACIÓN DE INFORMACIÓN DE REVOCACIÓN DISPONIBLES

Algunas PC pueden aceptar formas distintas a las antes descritas para la verificación de revocación, tales como los puntos de distribución de CRL (CDP).

11.7.10 CAUSAS PARA LA SUSPENSIÓN

La suspensión de la vigencia de los certificados se aplicará (en el caso de que dicha operación esté contemplada por la PC correspondiente), entre otros, en los siguientes casos:

- Cambio temporal de alguna de las circunstancias del titular del certificado que aconsejen la suspensión de los certificados mientras dure el mismo. Al retornarse a la situación inicial se levantará la suspensión del certificado. Las características y requisitos para la suspensión se establecerán en la correspondiente Política de Certificación.
- Comunicación por el titular del certificado de un posible compromiso de sus claves. En el caso de que la sospecha, por su grado de certeza, no aconseje la revocación inmediata, se suspenderán los certificados del titular mientras se averigua el posible compromiso de las claves.
- Por inhabilitación o cualquier circunstancia del titular del certificado que lo imposibiliten continuar en sus funciones.
- En los casos que la jefatura correspondiente lo estipuló oportuno previa solicitud de suspensión (aplicable a funcionario público).
- Las demás causales que establezcan en sus respectivas DPC.

11.7.10.1 QUIÉN PUEDE SOLICITAR LA SUSPENSIÓN

La solicitud puede presentarla el titular del certificado o la persona que se establezca en la PC correspondiente.

11.7.10.2 PROCEDIMIENTO PARA LA SOLICITUD DE SUSPENSIÓN

Cada PC establecerá el procedimiento para la solicitud de suspensión.

11.7.10.3 LÍMITES DEL PERIODO DE SUSPENSIÓN

Sin perjuicio de lo definido en las Políticas de Certificación, no se establece un plazo máximo de suspensión de la vigencia de los certificados.

Si durante el tiempo de suspensión del certificado éste caduca o se solicita su revocación, se producirán las mismas consecuencias que

para los Certificados no suspendidos en esos mismos casos de caducidad o revocación.

11.7.11 SERVICIOS DE INFORMACIÓN DEL ESTADO DE CERTIFICADOS

11.7.11.1 CARACTERÍSTICAS OPERATIVAS

La SAR-PKI pone a disposición de sus miembros el servicio de verificación mediante OCSP, el cual brinda información sobre el estado de los certificados emitidos por la CA:

- La Autoridad de validación pone a disposición la información de estado mediante el protocolo OCSP, el cual permite la verificación del estado de un certificado sin necesidad de consultar la CRL.
- Las listas CRL, serán publicadas en los repositorios, el acceso a las mismas debe realizarse por medio del protocolo HTTP.

11.7.11.2 DISPONIBILIDAD DEL SERVICIO

El o los servicios dispuestos para la verificación de estado de los certificados se encontrarán en línea con una disponibilidad mínima del 95% de manera anual, tanto para los suscriptores de los certificados como para los terceros que confían y/o las partes que lo requieran.

11.7.11.3 CARACTERÍSTICAS ADICIONALES

La SAR-PKI no es responsable por la provisión o entrega de un cliente OCSP para el uso del servicio de validación, es deber de quien desee hacer uso de dicho servicio obtener un cliente compatible con OCSP que esté en cumplimiento con la RFC2560.

11.8 CONTROLES DE INSTALACIONES, GESTIÓN Y OPERACIONALES

Con la finalidad de reforzar la confiabilidad y seguridad de las operaciones como Prestador de Servicio de Certificación, la Dirección Nacional de Tecnología del Servicio de Administración de Rentas, se ha encargado de la implementación de controles de seguridad física y lógica en todas sus instalaciones, de igual forma se han puesto en práctica procedimientos de auditoría interna e independiente, con el fin de llevar el seguimiento y verificación del cumplimiento de los procedimientos y políticas basados en las mejores prácticas de seguridad.

11.8.1 CONTROLES FÍSICOS

11.8.1.1 UBICACIÓN FÍSICA Y CONSTRUCCIÓN

La infraestructura tecnológica de la PKI se encuentra resguardada por medidas de seguridad de control de acceso, lo que garantiza que solo tendrán acceso a esta las personas que sean debidamente autorizadas.

Los IDC (Internet Data Center) en los que se hospeda la PKI, deben disponer como mínimo de los siguientes aspectos de seguridad física:

- Sistema interrumpible de energía (UPS).
- Sistema de UPS redundante.
- Sistema de enfriamiento de precisión.
- Sistema de detección de incendios
- Herramientas para la extinción de incendios.
- Sistema de monitoreo de infraestructura.
- Suministro de energía eléctrica regulada y con protección.
- Seguridad física 24/7.
- Sistema CCTV.

11.8.1.2 ACCESO FÍSICO

La infraestructura de la PKI consta de un perímetro seguro en el cual se ejecutan las operaciones más sensitivas, los controles de acceso incluyen por lo menos uno de los siguientes requisitos de acceso:

- Control Acceso Biométrico.
- Tarjetas RFID de Proximidad.

11.8.1.3 ELECTRICIDAD Y ACONDICIONADOR DE AIRES

- Suministro eléctrico:
  - PDU redundante.
  - UPS Redundante: Sistema Ininterrumpido de Energia.
- Aire acondicionado:
  - Sistema de enfriamiento de Aire de precisión.

11.8.1.4 EXPOSICIÓN AL AGUA

- Sistemas de drenaje y piso elevado.

11.8.1.5 PREVENCIÓN Y PROTECCIÓN DE INCENDIOS

Los recintos donde se encuentran ubicados los activos pertenecientes a la PKI del Servicio de Administración de Rentas disponen de dispositivos para la detección de incendios y dispositivos adecuados la extinción de estos. El cableado debe ser instalado en piso falso o techo falso.

11.8.1.6 EQUIPOS DE ALMACENAMIENTO

La información es manejada y almacenada en los medios de forma segura, de acuerdo con la clasificación de la información en ellos almacenada.

11.8.1.7 MANEJO DE RESIDUOS

La politica de almacenamiento seguro está dispuesta de manera que los procedimientos para la eliminación de residuos garantizan la eliminación de cualquier material que pudiera contener información.

11.8.1.8 RESPALDO EN SITIO ALTERNO

La SAR-PKI realiza respaldos de rutina de sistemas de datos criticos, datos de registro de auditoria y otra información sensitiva. El respaldo externo de medios se encuentra almacenado de una manera fisicamente segura utilizando las instalaciones de recuperación de la SAR-PKI.

11.8.2 CONTROLES DE PROCEDIMIENTO

En esta sección solo se incluye parte de los procedimientos de control, ya que los mismos son considerados de carácter confidencial y por motivos de seguridad se aconseja la no divulgación de estos.

La SAR-PKI es responsable de asegurar que la gestión de los procedimientos operacionales y administrativos, sean ejecutados de manera segura, en cumplimiento con lo establecido a este documento, realizando auditorias periódicas.

Se han establecido controles para la segregación de funciones, de manera que se evite el control de la totalidad de la infraestructura por una sola persona.

11.8.2.1 ROLES DE SAR-PKI

A continuación, enumeraremos los roles establecidos para el control y gestión del sistema.

a) Roles de gestión de los módulos de seguridad hardware (HSM)

- **Custodios de claves maestras:** Tienen en smartcards la información de la clave maestra con la que se inicializa el HSM. Esta clave maestra protege las claves de aplicación.

- **Custodios de claves de administración:** Tienen en smartcards la información que sirve para entrar en el modo de administración del HSM.

b) Roles de gestión de la SAR-PKI

- **Operador de certificados:** Grupo de usuarios responsables de las tareas de generación, Suspensión y revocación de los certificados.

- **Administrador de seguridad**: Grupo de usuarios cuya responsabilidad comprende la administración de la implementación de las políticas y prácticas de seguridad

- **Administrador de Sistema:** Grupo de usuarios con nivel de autorización para realizar las tareas de instalación, configuración y mantenimiento de las

entidades de la PKI, sin embargo, su acceso es limitado a la información relacionada a los parámetros de seguridad.

- **Operador de Sistema:** grupo de usuarios encargados de la realización de tareas diarias, las cuales no requieran de privilegios de administración, sin embargo, su acceso es limitado a la información relacionada a los parámetros de seguridad.

- **Auditor:** Grupo de usuarios responsables de llevar a cabo la verificación periódica con fines de auditoria sobre los archivos, logs y trazas de los componentes informáticos de la PKI.

11.8.2.2 NÚMERO DE PERSONAS REQUERIDAS POR TAREA

Será requisito asignar a un mínimo de dos personas para realizar operaciones relacionadas al rol de Administrador de Seguridad sobre la SAR-PKI, sin embargo, las demás tareas podrán ser realizadas por un miembro del equipo.

11.8.2.3 ROLES QUE REQUIEREN SEGREGACIÓN DE FUNCIONES

Para garantizar la separación de funciones y cualquier conflicto de intereses, los roles de HSM son incompatibles con los de los roles del Software de PKI, por lo cual un funcionario perteneciente a un grupo no debe ser asignado a tareas de su contraparte.

11.8.3 CONTROLES DE PERSONAL

11.8.3.1 APTITUD, CONOCIMIENTO Y ACREDITACIÓN DE PROFESIONALES

El recurso humano designado a labores de confianza en la SAR-PKI, debe tener la experiencia y aptitudes necesarias en relación con los servicios de certificación e infraestructura de clave pública, deben también estar en

cumplimiento con los requerimientos de la política de seguridad de la información y poseer conocimiento de lo siguiente:

- Fundamentos y experiencia en firma electrónica y certificados electrónicos.
- Adiestramiento específico para la función que desempeña.
- Título académico o experiencia equivalente.

11.8.3.2 PROCESO PARA COMPROBACIÓN DE ANTECEDENTES

La Dirección Nacional de Tecnología del Servicio de Administración de Rentas, es responsable de establecer los procesos para la verificación de la experiencia y aptitudes del recurso humano designado a tareas de confianza, a través de la oficina de Recursos Humanos de Servicio de Administración de Rentas, como parte del procedimiento se debe verificar:

- Verificación de empleos anteriores.
- Título académico y cursos o certificaciones obtenidas.
- Comprobación de conocimientos específicos.

11.8.3.3 REQUERIMIENTOS DE ENTRENAMIENTO

El recurso humano de Dirección Nacional de Tecnología debe estar en constante formación específica, la misma debe ser estipulada en un Plan anual de formación avalado por Servicio de Administración de Rentas, el cual debe incluir lo siguiente:

- Definiciones y Conceptos básicos de PKI.
- Medidas de Seguridad lógica y física de la operación.
- Tipos de servicios prestados por la Autoridad de Certificación.
- Aspectos legales relativos a la prestación de servicios de certificación.
- Declaración de Prácticas de Certificación.
- Técnicas de operación, administración y mantenimiento para cada rol específico.
- Gestión de incidencias.
- Técnicas para la continuidad del negocio en caso de desastres, para cada rol específico.

11.8.3.4 REQUERIMIENTOS Y FRECUENCIA DE REENTRENAMIENTO

El recurso humano de la Dirección Nacional de Tecnología debe estar en constante actualización de su currículo de formación, lo cual debe obedecer a cambios en las tecnologías o sistemas de seguridad, nuevas herramientas introducidas, cambios en los procedimientos operativos, cambios en la DPC o documentos relacionados a la gestión y funcionamiento de la SAR-PKI.

11.8.3.5 FRECUENCIA Y SECUENCIA DE ROTACIÓN DE OBLIGACIONES

Con la finalidad de garantizar la continuidad del negocio y la seguridad operativa, la Dirección Nacional de Tecnología, estipulará rotaciones periódicas de trabajo para el personal entre los diversos roles descritos en este documento. Antes de ejercer un nuevo rol, el individuo debe recibir la capacitación necesaria que asegure el correcto desempeño de las tareas del nuevo rol específico.

11.8.3.6 SANCIONES POR ACCIONES NO AUTORIZADAS

Las sanciones y procedimientos que seguir para el cumplimiento de estas serán definidas en el reglamento interno de Servicio de Administración de Rentas (RECAEFUSAR)

11.8.3.7 REQUISITOS DE CONTRATACIÓN DE TERCEROS

La Dirección Nacional de Tecnología estará en la potestad de realizar contrataciones de recursos externos a la entidad atreves del área encargada siempre y cuando exista una relación claramente establecida con el contratista y cuando se cumplan las siguientes circunstancias:

- Existe un documento contractual que define clausulas especificas a los roles de gestión y estipula penalizaciones para las acciones no autorizadas.
- La Dirección Nacional de Tecnología no cuenta con la disponibilidad del recurso humano para ejercer los roles contratados.

- Los contratistas deben cumplir con los requisitos estipulados en el punto 6.8.3.1. aptitud, conocimiento y acreditación de profesionales.
- Al momento de finalizar la relación contractual con el contratista se debe realizar la revocación y baja respectiva de los usuarios y accesos.

11.8.3.8 DOCUMENTACIÓN PROVISTA AL PERSONAL

La Dirección Nacional de Tecnología, dotará a todo su personal de la información, documentación y buenas prácticas de seguridad de la información indispensables para el correcto cumplimiento de sus tareas y obligaciones, la documentación debe incluir, pero no restringirse a:

- Declaración de Prácticas de Certificación.
- Técnicas de instalación, operación, mantenimiento y gestión de la SAR-PKI de según los roles específicos.
- Política de Seguridad de la Información.
- Modelo de Gobernanza de TI.
- Procedimientos de Continuidad del negocio.
- Gestión de incidencias.
- Otros documentos necesarios

11.8.4 PROCEDIMIENTOS DE AUDITORÍA DE REGISTROS

11.8.4.1 TIPOS DE EVENTOS REGISTRADOS

La SAR-PKI emplea herramientas o mecanismos con el fin de registrar entre otros, los eventos descritos a continuación.

- Inicios de Sesión a componentes de la PKI
- Modificación de Políticas de Certificación.
- Modificación de Roles.
- Generación de Solicitudes de certificación.

Por cada evento se registrará:

- Descripción del evento
- Operador relacionado a la acción que disparó el evento
- Fecha de ejecución.
- Toda esta información puede ser consultada:

Mediante la Interfaz de administración de cada componente de la PKI, realizando la autenticación con el Rol de Auditor.

11.8.4.2 FRECUENCIA DE PROCESADO DE REGISTROS

Los registros serán analizados de forma periódica, mediante las auditorias de la PKI, también podrán ser realizada a demanda, de ser necesario.

11.8.4.3 PERÍODO DE RETENCIÓN DE LOS REGISTROS DE AUDITORÍA

La totalidad de la información generada en los registros de eventos deberá ser mantenida en:

- En la base de datos de la PKI, por la totalidad del periodo de vida de la PKI.

11.8.4.4 PROTECCIÓN DE LOS REGISTROS DE AUDITORÍA

En todo momento deben implementarse las medidas necesarias que garanticen la Integridad y disponibilidad de los registros de auditoria, de manera que los mismos sean accesibles al momento de ser necesarios.

11.8.4.5 PROCEDIMIENTOS DE RESPALDO DE LOS REGISTROS DE AUDITORIA.

Respaldos incrementales de registros de auditoría son creados y respaldados diariamente.

11.8.4.6 ANÁLISIS DE VULNERABILIDADES.

Los eventos en el proceso de auditoria son registrados, en parte, para monitorear las vulnerabilidades del sistema. Evaluaciones de vulnerabilidad de seguridad son realizadas, repasadas y revisadas. Las mismas se encuentran basadas en datos registrados automáticamente en tiempo real y son respaldadas a diario.

11.8.5 ARCHIVADO DE REGISTROS

11.8.5.1 TIPO DE EVENTOS ARCHIVADOS

La SAR-PKI preservará la totalidad de la información relevante sobre las operaciones realizadas sobre los certificados durante el periodo de tiempo

establecido en este documento, los datos almacenados incluirán, pero no se limitarán a los siguientes:

- Datos correspondientes a los procedimientos de inscripción y emisión de los certificados.
- Datos correspondientes a los cambios de estado de certificados tales como la suspensión, revocación, etc.

11.8.5.2 PERÍODO DE CONSERVACIÓN DE REGISTROS

La totalidad de la información y documentación correspondiente a los certificados será resguardada durante un periodo no menor a 7 años.

11.8.5.3 PROTECCIÓN DEL ARCHIVO

La totalidad de la documentación digital y fisica que sea generada como resultado de los procedimientos propios de la PKI, serán almacenado de forma segura en las instalaciones de Servicio de Administración de Rentas, haciendo uso de los controles de acceso pertinentes.

11.8.5.4 PROCEDIMIENTOS DE COPIA DE RESPALDO DEL ARCHIVO

Las copias de respaldo de los archivos se llevan a cabo siguiendo lo estipulado en los procedimientos de respaldo definidos por la Dirección Nacional de Tecnología.

11.8.5.5 PROCEDIMIENTOS PARA OBTENER Y VERIFICAR INFORMACIÓN ARCHIVADA

Los archivos de eventos registrados se encuentran con acceso protegido, asegurando que solo puedan ser accedidos por las aplicaciones dispuestas para su visualización y gestión. El personal autorizado tendrá acceso a los archivos fisicos de soportes y archivos informáticos, con el fin de ser capaces de verificar la integridad, entre otros aspectos.

11.8.6 CAMBIO DE CLAVES

Los procedimientos para llevar a cabo el cambio de clave, por una nueva clave pública de AC y proporcionarla a los suscriptores y terceros que confian de los certificados de la AC, son los mismos que fueron utilizados para

proporcionar la clave pública en vigencia. Por lo tanto, la clave pública será publicada en el repositorio de SAR-PKI.

11.8.7 RECUPERACIÓN POR COMPROMISO DE CLAVE O CATÁSTROFE

11.8.7.1 RECUPERACIÓN EN SITIO ALTERNO POR DESASTRE NATURAL

Se describen los requerimientos relativos a la recuperación de los recursos de la PKI-SAR en caso de falla o desastre. Estos requerimientos serán desarrollados en el Plan de Continuidad de Negocio (BCP).

Se han desarrollado procedimientos referidos a:

- Plan de respuesta a los incidentes.
- Registro de incidentes
- Plan de recuperación ante desastres
- Manual de respaldo de PKI-SAR
- Recuperación ante falla inesperada o sospecha de falla de componentes de hardware, software y datos.

Los procedimientos cumplen con lo establecido por el artículo 23 del Reglamento de la Ley Sobre Firmas Electrónicas Acuerdo Ejecutivo No. 41-2014, en lo relativo a la existencia de un plan en caso de emergencia.

11.8.7.2 PROCESO DE RESPUESTA ANTE EL COMPROMISO DE LA CLAVE PRIVADA DE UNA AUTORIDAD

De darse el compromiso de la clave privada de una Autoridad, se revocará la misma inmediatamente, y se procederá a la generación y publicación de la ARL. Se finalizará el funcionamiento de la actividad de la autoridad comprometida y se realizará la generación, certificación y puesta en marcha de una nueva autoridad con la misma jerarquía y características que la cesante, haciendo uso de un nuevo par de claves.

Se emitirá un comunicado a todas las Autoridades afectadas indicando que todos los certificados y la información sobre su revocación, como resultado del uso de la clave comprometida de la AC, carece de validez a partir de emitida la notificación, debiendo utilizar para verificar la validez de la información, la nueva clave pública de la AC. Las Autoridades tienen la

obligación de solicitar un nuevo certificado a la AC una vez que ésta última disponga de un nuevo par de claves.

Serán revocados los certificados que hayan sido firmados por Autoridades dependientes de la AC afectada en el lapso comprendido entre el compromiso de la clave y la revocación del certificado en cuestión.

11.8.8 CESE DE UNA AC O AC

11.8.8.1 AUTORIDAD DE CERTIFICACIÓN

En el caso de cese de actividad de alguna de las AC del Servicio de Administración de Rentas, es responsabilidad de Dirección Nacional de Tecnología informar a cada firmante, con un plazo mínimo de noventa (90) días de anticipación a la fecha de la cesación efectiva de actividades sobre la finalización de prestación de servicio. Es imperativo que la notificación especifique la fecha de la cesación efectiva de actividades, de igual forma, los motivos por los cuales se procede a tal cese.

Igualmente, los certificados que continúen vigentes podrán ser traspasados a otro prestador de servicios de certificación, previo consentimiento del firmante y por cuenta del prestador de servicios de certificación o en caso contrario, los mismos serán revocados.

Si al momento del cese de actividades por parte de SAR-PKI el certificado electrónico de un Suscriptor tiene plazo de vigencia pendiente de uso mayor a seis (6) meses, el Servicio de Administración de Rentas tendrá la obligación de reembolsar el importe de la tarifa acorde a la vigencia no utilizada a menos que dicho certificado haya sido traspasado a otro Prestador de Servicios de Certificación.

11.8.8.2 AUTORIDAD DE REGISTRO

Al momento en que la Autoridad de Registro cese sus actividades, traspasará los registros que mantenga a SAR-PKI, mientras exista la obligación de mantener archivada la información, de lo contrario, ésta será destruida.

11.9 CONTROLES DE SEGURIDAD TÉCNICA

En el contexto de la presente DPC se especificarán los detalles correspondientes a las claves de las autoridades de certificación. Los detalles correspondientes a las claves de los Suscriptores de los certificados se podrán consultar en la Política de Certificación que corresponda de acuerdo con el tipo de certificado.

11.9.1 GENERACIÓN E INSTALACIÓN DEL PAR DE CLAVES

11.9.1.1 GENERACIÓN DEL PAR DE CLAVES

Los pares de llaves correspondientes a los componentes internos de SAR-PKI, especificamente CA Raíz y las AC Subordinadas, serán generados en módulos de hardware criptográficos con certificación FIPS 140-2 Nivel 3 que tienen instalados en sus respectivos sistemas.

Los pares de llaves para el resto de los suscriptores se generan de acuerdo de lo dispuesto en la Política de Certificación correspondiente a cada certificado.

Los dispositivos hardware o software para utilizar en la creación de claves para cada tipo de certificado emitido por SAR-PKI son estipulados por la Política de Certificación correspondiente a cada certificado.

11.9.1.2 ENTREGA DE LA LLAVE PRIVADA AL SUSCRIPTOR

El procedimiento para la entrega de la clave privada a sus Suscriptores es propio de cada certificado y será establecido en la Política de Certificación correspondiente a cada certificado.

11.9.1.3 ENTREGA DE LA CLAVE PÚBLICA AL EMISOR DEL CERTIFICADO

El procedimiento para la entrega de la clave pública al emisor en los casos en que sea generada por el Suscriptor dependerá de cada certificado y será establecido en la Política de Certificación correspondiente a cada certificado.

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

La clave pública de las CA de SAR-PKI está a disposición de los terceros que confían, en el Repositorio de SAR-PKI (ver apartado 2.1) sin perjuicio de que una PC pueda establecer procedimientos complementarios para la entrega de dichas claves.

11.9.1.5 TAMAÑO DE LAS CLAVES

El Tamaño de claves está estipulado de la siguiente manera:

- AC y AC Subordinadas= RSA 4096 bits SHA-256
- Certificados de suscriptores = RSA 2048 bits SHA256

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

La clave pública de la AC de SAR-PKI está codificada en consonancia con RFC 5280 y PKCS#1. El algoritmo empleado para la generación de claves es RSA.

Los parámetros de generación de claves para cada tipo de certificado emitido por SAR-PKI son estipulados por Política de Certificación correspondiente a cada certificado.

Las técnicas y medios de comprobación de la calidad de los parámetros usados para la generación de claves para cada tipo de certificado emitido por SAR-PKI son estipulados por Política de Certificación correspondiente a cada certificado.

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

Los usos permitidos de la clave para cada tipo de certificado emitido por SAR-PKI son estipulados por Política de Certificación correspondiente a cada certificado.

La totalidad de los certificados emitidos por SAR-PKI incluyen la extensión Key Usage definida por el estándar X.509 v3, los valores empleados en este campo corresponden a los especificados en el RFC6487. Igualmente, pueden establecerse otros usos o restricciones utilizando la extensión Extended Key Usage.

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

11.9.2.1 ESTÁNDARES PARA LOS MÓDULOS CRIPTOGRÁFICOS

Los módulos empleados para la emisión de claves usadas por las AC de SAR-PKI deben cumplir con la certificación FIPS 140-2 de nivel 3.

La puesta en marcha de cada una de las Autoridades de Certificación, tomando en consideración que debe utilizar un módulo Criptográfico de seguridad (HSM), implica lo siguiente:

- Inicialización de estado del módulo criptográfico
- Creación de las claves para los usuarios de los siguientes roles
  - Operador de certificados
  - Administrador de seguridad
  - Administrador de sistema
  - Operador de sistema
- Generación de las claves de la AC.

La SAR-PKI emplea módulos criptográficos hardware y software disponibles comercialmente desarrollados por terceros.

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

Las claves privadas de las ACs están protegidas criptográficamente por la clave maestra del HSM. Esta clave maestra se encuentra respaldada entre varios custodios en dispositivos criptográficos, y se requiere la participación de varios de ellos para su recomposición.

11.9.2.3 RESGUARDO DE LA CLAVE PRIVADA

Las claves privadas de las Autoridades de Certificación que conforman SAR-PKI son resguardadas en dispositivos de hardware criptográfico con certificación FIPS-2 de nivel 3 enlazadas a las distintas ACs.

11.9.2.4 RESPALDO DE LA CLAVE PRIVADA

Se hará respaldo de la clave maestra del HSM a través de las interfaces de administración de la PKI. Esta clave y el backup están criptográficamente protegidas por la clave maestra del HSM.

11.9.2.5 ARCHIVO DE LA CLAVE PRIVADA

Referirse a los numerales 11.9.2.3 y 11.9.2.4.

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

La transferencia de la clave privada puede ser realizada únicamente entre módulos criptográficos (HSM) y requiere de la actuación de un mínimo de dos (2) **custodios de claves maestras** y administradores de seguridad.

11.9.2.7 ALMACENAMIENTO DE LA CLAVE PRIVADA EN UN MÓDULO CRIPTOGRÁFICO

Las claves privadas se originan en el módulo criptográfico en el momento de la creación de cada una de las Autoridades de SAR-PKI que utilizan dichos módulos y se almacenan cifradas.

11.9.2.8 MÉTODO DE ACTIVACIÓN DE LA CLAVE PRIVADA

Este numeral se define como "No Estipulado" ya que no existe el concepto de activación en la clave privada del HSM.

11.9.2.9 MÉTODO DE DESACTIVACIÓN DE LA CLAVE PRIVADA

Este numeral se define como "No Estipulado" ya que no existe el concepto de activación o desactivación en la clave privada del HSM

11.9.2.10 MÉTODO DE DESTRUCCIÓN DE LA CLAVE PRIVADA

En el caso de los certificados de personas como se establezca en la Política de Certificación correspondiente a cada certificado.

11.9.2.11 CLASIFICACIÓN DE LOS MÓDULOS CRIPTOGRÁFICOS

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

11.9.3 OTROS ASPECTOS DE LA ADMINISTRACIÓN DEL PAR DE CLAVES

11.9.3.1 ARCHIVO DE LA CLAVE PÚBLICA

Es Responsabilidad de SAR-PKI mantener un archivo de todos los certificados, los cuales deben incluir las claves públicas, emitidos por un periodo mínimo de, siete (7) años. El control de dicho registro es deber de los Administradores de cada una de las ACs de SAR-PKI. El sistema mantendrá

la cabalidad de la integridad, confidencialidad y disponibilidad de las claves públicas empleando los medios necesarios para garantizar que no existan manipulaciones a la misma.

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

El certificado y par claves de la Autoridad Certificadora tiene una validez de cinco (5) años.

El periodo de validez del resto de certificados vendrá establecido en las políticas de certificación que corresponda.

11.9.4 DATOS DE ACTIVACIÓN

11.9.4.1 INSTALACIÓN Y GENERACIÓN DE LOS DATOS DE ACTIVACIÓN

Para la instalación de una Autoridad de Certificación es necesaria la creación de tarjetas criptográficas, cuya utilidad será empleada en actividades de recuperación y funcionamiento. El HSM opera con 2 tipos de roles, cada uno con sus tarjetas criptográficas correspondientes:

- Tarjetas de custodios de claves maestras
- Tarjetas de custodios de administración

En caso de daño, perdida física o pérdida del PIN por el custodio, el conjunto de tarjetas debe ser clonado nuevamente a la brevedad posible, empleando para este propósito las tarjetas correspondientes.

11.9.4.2 PROTECCIÓN PARA DATOS DE ACTIVACIÓN

Únicamente el personal autorizado tendrá acceso a los datos para poner en funcionamiento la AC. Para esto tendrán en su posesión las tarjetas criptográficas con capacidad de recuperación de las AC y conocerán los PIN y contraseñas necesarios.

11.9.4.3 OTROS ASPECTOS REFERENTES A LOS DATOS DE ACTIVACIÓN

No estipulado.

11.9.5 CONTROLES DE SEGURIDAD INFORMÁTICA

Los datos referentes a este numeral son considerados información confidencial, por lo tanto, se proporcionan únicamente a quien acredite la necesidad de conocerlos, como en el caso de auditorias externas o internas e inspecciones.

11.9.6 CONTROLES TÉCNICOS DE CICLO DE VIDA

Los datos referentes a este numeral son considerados información confidencial, por lo tanto, se proporcionan únicamente a quien acredite la necesidad de conocerlos.

11.9.6.1 CONTROLES DE DESARROLLO DE SISTEMA

Es de carácter mandatorio el aplicar las condiciones de seguridad necesarias durante todo el ciclo de desarrollo de la PKI, ya que esto influye sobre la seguridad de todo el sistema.

11.9.6.2 CONTROLES DE ADMINISTRACIÓN DE SEGURIDAD

Es imperativo que el SAR-PKI lleve a cabo el levantamiento y mantenimiento de un inventario de activos tecnológicos, ya que esto asegura y permite la debida clasificación de los activos, lo que permitirá una mejor gestión de seguridad.

11.9.6.3 CONTROLES DE SEGURIDAD DEL CICLO DE VIDA

Se han dispuesto controles de seguridad a lo largo de todo el ciclo de vida de los sistemas que tengan algún impacto en la seguridad de SAR-PKI.

11.9.7 CONTROLES DE SEGURIDAD DE REDES

Los datos referentes a este numeral son considerados información confidencial, por consiguiente, solo serán revelados a entidades autorizadas.

11.9.8 SELLADO DE TIEMPO

El Sellado de Tiempo no será implementado en la SAR-PKI, por lo tanto, se considera este numeral como "no aplicable".

11.10 CONSIDERACIONES DE OCSP, CRL Y CERTIFICADOS

11.10.1 PERFIL DE CERTIFICADO

11.10.1.1 NÚMERO DE VERSIÓN

SAR-PKI es compatible con certificados X.509 versión 3 (X.509 v3)

11.10.1.2 ISSUER

El campo Issuer se refiere al DN de la CA que firmó y por ende genera la CRL.

11.10.1.3 VALIDITY

El campo Validity provee dos atributos que son notBefore (FECHA DE EMISION) y notAfter (FECHA DE EXPIRACIÓN), los cuales definen el período de tiempo durante el cual el certificado es válido.

11.10.1.4 SUBJECT

El campo Subject se refiere al DN que define la entidad asociada con el certificado.

11.10.1.5 SUBJECTPUBLICKEYINFO

El campo SubjectPublicKeyInfo provee dos atributos, algoritmo y clave pública.

11.10.1.6 EXTENSIONES

a) BasicConstraints

El Campo Basic identifica si el sujeto del certificado se trata de una CA o no y define la profundidad de la cadena de confianza. Se considera como una extensión crítica.

b) CertificatePolicies

El campo CertificatePolicies es utilizado para identificar las políticas particulares del Issuer. Se considera como una extensión no crítica.

a. Identificador de objeto (OID) de la Política de Certificación tal como estipule la PC correspondiente.

SAR-PKI deberá asignar los OID de las mismas dentro del rango de numeración de la SAR-PKI, por lo cual el OID de todas las extensiones propietarias de Certificados del SAR-PKI comienzan con el prefijo 2.16.340.1.1 Se considera como una extensión no crítica.

c) SubjectAlternateNames

El campo SubjectAlternateNames es utilizado para definir los campos adicionales de identificación del individuo citados en la Ley sobre firma electrónica Decreto No. 149-2013, publicado en el Diario Oficial la Gaceta el 11 de diciembre de 2013. Se considera como una extensión no critica.

d) AuthInformationAccess

El campo AuthInformationAccess es utilizado para definir la ruta de consulta del servicio de verificación en línea de estado del certificado. Se considera como una extensión no crítica.

e) KeyUsage

El campo KeyUsage es utilizado para listar los usos principales del certificado. Se considera como una extensión critica.

f) ExtendedKeyUsage

El campo ExtendedKeyUsage es utilizado para listar los usos complementarios del certificado. Se considera como una extensión no crítica.

g) CRL Distribution Point

Este campo contiene la url del punto de distribución de CRL. Se considera como una extensión no crítica.

11.10.1.7 IDENTIFICADORES DE OBJETO (OID) DE LOS ALGORITMOS

OID de los algoritmos Criptográficos: SHA-256 with RSA Encryption (1.2.840.113549.1.1.11)

11.10.2 MÉTODOS DE VERIFICACIÓN DE REVOCACIÓN

Los métodos empleados para la verificación de estado o revocación de los certificados serán el Protocolo OCSP o las CRL.

11.10.2.1 DEFINICIÓN DE PROTOCOLO OCSP

Cumpliendo con el RFC 2560, el protocolo OCSP permite que aplicaciones puedan determinar el estado (revocación) de un certificado. OCSP puede ser empleado para satisfacer requerimientos operacionales en los cuales sea necesario proveer una vía con mayor rapidez y certeza sobre la información de revocación de lo actualmente posible con las CRL, además de que este protocolo provee de información de estado adicional.

El Cliente OCSP debe emitir una solicitud de estado hacia un ente verificador o OCSP Responder, en este momento se suspende la aceptación del certificado en cuestión hasta que sea verificada la solicitud y emitida una respuesta por parte del verificador.

a) Solicitud de Verificación

Una solicitud de OCSP deberá contener la siguiente información:

- Versión
- Solicitud de servicio
- Identificador del certificado a consultar

Al momento de recibir la solicitud el Validador OCSP deberá determinar lo siguiente

- Determinar si el mensaje lleva la estructura correcta
- Determinar si el validador OCSP se encuentra configurado para proveer servicio a las solicitudes

- Determinar si el mensaje contiene la información necesaria por el Validador OCSP

En caso de que alguna de las estipulaciones anteriores no sea cumplida, el validador devolverá un mensaje de error, de caso contrario enviará una respuesta definitiva.

b) Respuesta

En el protocolo OCSP las respuestas constan de dos partes, el tipo de respuesta y los bytes que comprenden la respuesta en si, a continuación, detallaremos las características básicas de una respuesta OCSP.

Todas las respuestas definitivas deben ser firmadas digitalmente. La Clave utilizada para firmar dicha respuesta debe pertenecer a una de las siguientes entidades:

- La AC que emitió el certificado en cuestión
- Un validador OCSP autorizado cuya clave pública es de confianza para el solicitante de la verificación
- Una Autoridad de Validación, designada por la AC.

El mensaje de la respuesta definitiva debe ser compuesto de:

- Versión de la sintaxis de respuesta.
- Nombre del Validador
- Respuestas por cada certificado enviado en la solicitud
- Extensiones opcionales
- OID de algoritmo de firma
- Firma calculada mediante el hash de la respuesta

La respuesta para cada uno de los certificados contenidos en la solicitud debe constar de:

- Identificador de Certificado
- Valor de Estado de Certificado
- Lapso de validez de la respuesta
- Extensiones opcionales

Los valores utilizados para definir el Valor de Estado del Certificado deben ser:

- Bueno: Indica una respuesta positiva a la consulta de estado
- Revocado: indica que el certificado ha sido revocado ya sea de forma permanente o temporalmente (suspendido).
- Desconocido: indica que el validador no reconoce el certificado en cuestión.

c) Extensiones OCSP

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

11.10.2.2 **CONSIDERACIONES DE CRL**

Cada CA debe emitir CRLs de versión 2 lo cual obedece al RFC5280. Es imperativo que las CRL sean emitidas por la CA, ya que el alcance de la CRL debe ser la totalidad de los certificados emitidos por dicha AC.

En el caso de que dos o más CRL hayan sido emitidas por la misma AC, la CRL con el mayor valor en el campo de "Numero de CRL" (CRL Number), reemplazará a todas las demás CRL emitidas por la AC en cuestión.

El contenido de la CRL comprende una lista de todos los certificados no expirados que han sido revocados por la AC.

11.11 **AUDITORÍAS DE CUMPLIMIENTO Y OTROS CONTROLES**

Las auditorias son un aspecto crítico en el correcto funcionamiento dentro de una PKI, por lo cual la SAR-PKI deberá ser sujeto de Auditorías con una frecuencia no menor a doce (12) meses.

Dichas auditorias deben ser ejecutadas por empresas auditoras externas. El recurso humano designado para realizar una auditoría de seguridad a la SAR-PKI deberá cumplir los siguientes requisitos:

- Experiencia y formación de alto nivel en cuanto, seguridad, tecnologías criptográficas y procesos de auditoría.

- No depender de ninguna manera a nivel organizativo de la autoridad de SAR-PKI.

La auditoria debe como mínimo cubrir los siguientes aspectos:

- DPC y PC competentes
- Evaluación de Infraestructura y controles tecnológicos.
- Administración de los servicios de la AC
- Políticas de seguridad y privacidad
- Controles de Recurso Humano
- Remediación de hallazgos

Una vez finalizada la auditoria, el ente equipo auditor comunicará los resultados de la auditoria a la Autoridad Administrativa Competente de SAR-PKI (AAC), al Gestor de Seguridad de SAR-PKI, así como a los administradores de SAR-PKI y de la Autoridad en la que se detecten incidencias. Los resultados de las auditorias deben ser comunicados a la brevedad posible a la Autoridad Administrativa Competente, al Gestor de Seguridad de, así como a los administradores de la SAR-PKI y de la Autoridad en la que se detecten anomalías.

Se pueden realizar auditorias extraordinarias por parte AAC para asegurar que se han respetado las condiciones establecidas para la acreditación de SAR-PKI como Prestadora de Servicios de Certificación (PSC).

11.12 OTROS ASPECTOS LEGALES Y DE ACTIVIDAD

11.12.1 9.1 TARIFAS

11.12.1.1 TARIFAS PARA EMISIÓN O RENOVACIÓN DE CERTIFICADO

Las tarifas de emisión y renovación de cada certificado son estipuladas en la Política de Certificación que corresponda.

11.12.1.2 TARIFAS PARA ACCESO A CERTIFICADOS

Las tarifas de acceso a los certificados son estipuladas en la Política de Certificación que corresponda.

11.12.1.3 TARIFAS PARA ACCESO A INFORMACIÓN DE ESTADO O REVOCACIÓN

Las tarifas de acceso a la información de estado o revocación de cada certificado son estipuladas en la Política de Certificación que corresponda.

11.12.1.4 TARIFAS PARA OTROS SERVICIOS.

El acceso a la información de la presente DPC y PC correspondiente a cada certificado será de carácter gratuito, por lo que no existe tarifa asociada a su acceso. Sin embargo, esta estipulación podrá ser reemplazada por lo estipulado en su respectiva PC.

11.12.1.5 POLÍTICA DE REEMBOLSO

La política de reembolso aplicable debe ser definida por la PC correspondiente a cada tipo de certificado.

Si al momento del cese de actividades por parte de SAR-PKI el certificado electrónico de un Suscriptor tiene plazo de vigencia pendiente de uso mayor a seis (6) meses, el Servicio de Administración de Rentas tendrá la obligación de reembolsar el importe de la tarifa acorde a la vigencia no utilizada a menos que dicho certificado haya sido traspasado a otro Prestador de Servicios de Certificación.

11.12.2 RESPONSABILIDADES ECONÓMICAS

Este numeral no es estipulado ya que la Póliza de Responsabilidades económicas no es exigida para entidades gubernamentales.

11.12.3 CONFIDENCIALIDAD DE LA INFORMACIÓN

Toda la información que en conocimiento de Dirección Nacional de Tecnología como prestador de servicios de certificación en relación con los datos personales de sus usuarios debe ser mantenida en estricta confidencialidad. Así mismo todos sus funcionarios, proveedores, y contratistas deben mantener estricta confidencialidad de toda la información que adquieran o manejen, en relación con todos los elementos relacionados a la SAR-PKI.

11.12.3.1 ALCANCE DE LA INFORMACIÓN CONFIDENCIAL

Toda información que no esté explícitamente clasificada como pública por el Servicio de Administración de Rentas será tratada en adelante como confidencial. Esta información incluye, pero no se limita a:

- Las claves privadas de las Autoridades que componen SAR-PKI.
- La información sobre operaciones que lleve a cabo SAR-PKI.
- La información referente a los parámetros de seguridad, control y procedimientos de auditoría.

11.12.3.2 INFORMACIÓN FUERA DEL ALCANCE DE LA INFORMACIÓN CONFIDENCIAL

Se considera información pública y por lo tanto accesible por terceros:

- La presente Declaración de Prácticas de Certificación.
- Políticas de certificación.
- Los certificados emitidos por SAR-PKI.
- La lista de los certificados suspendidos o revocados.

11.12.3.3 RESPONSABILIDAD DE PROTEGER LA INFORMACIÓN CONFIDENCIAL.

El recurso humano de Dirección Nacional de Tecnología, del Servicio de Administración de Rentas y otros organismos externos a ellos que participen en cualesquiera tareas relacionadas a la operación de SAR-PKI están obligados al deber de secreto profesional y por lo tanto sujetos a la normativa aplicable del Reglamento Interno de Servicio de Administración de Rentas (RECAEFUSAR)

11.12.4 PRIVACIDAD DE LA INFORMACIÓN PERSONAL

La SAR-PKI se encuentra en la obligación de asegurar la protección, la confidencialidad y el debido uso de la información suministrada por los usuarios de los servicios de certificación de conformidad con la Constitución de la República de Honduras, en su artículo 76, garantiza el derecho al honor, la intimidad y a la imagen de toda persona.

11.12.5 DERECHOS DE PROPIEDAD INTELECTUAL

Los derechos de propiedad intelectual que puedan derivarse del sistema de certificación supeditado a esta DPC, es propiedad exclusiva del Servicio de Administración de Rentas. Por tal motivo se prohíbe cualquier reproducción, distribución o comunicado público que refiera al material antes citado, sin autorización expresa del Servicio de Administración de Rentas

11.12.6 OBLIGACIONES

11.12.6.1 OBLIGACIONES DE LAS ACS

Las AC que operan bajo la jurisdicción de SAR-PKI deben acogerse a las obligaciones dispuestas en este numeral, cada AC deberá prestar sus servicios de forma consistente con esta DPC

Las ACs que operan bajo la jerarquía de SAR-PKI tienen las siguientes obligaciones:

- Realizar sus operaciones en cumplimiento de esta DPC.
- Resguardar sus claves privadas.
- Emitir certificados en según lo estipulado en las Políticas de Certificación correspondientes.
- Posterior a la recepción de una solicitud válida de certificado, emitir certificados de acuerdo con el estándar X.509 v3 y con los requerimientos de la solicitud.
- Emitir certificados que sean fieles a la información conocida en el momento de su emisión, y libres de errores de entrada de datos.
- Publicar los certificados cuando sea necesario para interactuar con otros usuarios o sistemas informáticos que así lo requieran.
- Procesar las revocaciones de certificados según lo estipulado en la sección 6.7.9 Suspensión y Revocación de Certificados y publicar los certificados revocados en la CRL en el servicio de directorio y servicio Web mencionados en el apartado 2.1 Repositorio, con la periodicidad estipulada en el punto 6.7.9.7 Frecuencia de emisión de CRL
- Publicar esta DPC y las PC correspondientes en el sitio web referido en el apartado 6.5.1 Repositorio.
- Emitir Comunicados sobre los cambios de esta DPC y de las PC de

según lo estipula en el apartado 11.12.11 Notificaciones individuales y comunicaciones con los participantes

- Preservar los documentos de aceptación de condiciones de los servicios de certificación de la autoridad de certificación del Servicio de Administración de Rentas firmados, en papel o electrónicamente, con los solicitantes de certificados en los que estos aceptan sus obligaciones y derechos, admiten el tratamiento de sus datos personales por parte de la AC y confirman que la información proporcionada es fidedigna.
- Realizar las notificaciones sobre la revocación de certificados en conformidad con las Políticas de certificación correspondientes.
- Funcionar en consonancia con las leyes aplicables.
- Salvaguardar las claves bajo su custodia.
- No almacenar, ni copiar en ningún caso los datos de creación de firma, clave privada, de los Suscriptores de certificados emitidos con el propósito de utilizarse para firma electrónica.
- Mantener en todo momento la confidencialidad de la información propia de los suscriptores y suscriptores de certificado electrónico, delimitando su utilización solo a las tareas del servicio de certificación, salvo orden judicial o solicitud del suscriptor o suscriptor mismo.

11.12.6.2 **OBLIGACIONES DE LAS ARS**

Las ARs operativas en SAR-PKI deben cumplir las siguientes obligaciones:

- Realizar la identificación del suscriptor o solicitante de acuerdo con lo estipulado en las PC correspondientes y lo que establece esta DPC.
- Formalizar la expedición de Certificados con el Suscriptor de acuerdo con lo estipulado en las PC correspondientes.
- Garantizar el almacenado de forma segura y por un plazo de tiempo razonable la documentación aportada en el proceso de emisión del certificado y en el proceso de suspensión/revocación de este.
- Ejecutar las funciones que han sido estipuladas en esta DPC.

11.12.6.3 **OBLIGACIONES DE LOS SUSCRIPTORES DE LOS CERTIFICADOS.**

Es obligación de los Suscriptores de los certificados emitidos bajo la presente DPC:

- Proporcionar información fidedigna, completa y veraz según los datos solicitados en el proceso de verificación asociado al proceso de registro.
- Informar a los responsables de SAR-PKI sobre cualquier cambio de esta información.
- Conocer y aceptar las condiciones de utilización de los certificados, en particular las contenidas en esta DPC y en las PC correspondientes a cada caso.
- Hacer uso del certificado según lo estipulado por la Política de Certificación correspondiente a cada caso y la presente DPC.
- Custodiar su Clave Privada, evitando su pérdida, divulgación, modificación o uso no autorizado del mismo.
- Solicitar inmediatamente la suspensión o revocación de un certificado en el caso de detección de inexactitudes en la información contenida en el mismo o tener conocimiento o sospecha del compromiso de la clave privada correspondiente a la clave pública contenida en el certificado, entre otras causas por: pérdida, robo, compromiso potencial, conocimiento por terceros de la contraseña de su repositorio criptográfico PKCS12.
- No emprender actividades que tengan como finalidad el obtener información de ingeniería inversa sobre la implantación técnica (hardware y software) de los servicios de certificación
- No traspasar a un tercero sus responsabilidades sobre un certificado del cual es Suscriptor.
- Cualquier otra que se derive de la Ley Sobre Firmas Electrónicas, su reglamentación, de esta DPC o de las Políticas de Certificación.

11.12.6.4 OBLIGACIONES DE LOS TERCEROS QUE CONFÍAN O ACEPTEN LOS CERTIFICADOS

Es obligación de los terceros que aceptan y confian en los certificados emitidos por SAR-PKI:

- Limitar el empleo de los certificados a los usos permitidos de los mismos, según lo dispuesto en las extensiones de los certificados y la Política de Certificación que corresponda.
- Verificar la validez de los certificados en el momento de la recepción de los documentos firmados electrónicamente mediante la comprobación de que el certificado es válido y no ha caducado o ha sido suspendido o revocado.
- verificación de las firmas electrónicas.
- comprobación de la validez, revocación o suspensión de los certificados que acepta y en que confia.
- Tener conocimiento de las garantías y responsabilidades derivadas de la aceptación de los certificados en los que confía y aceptar sujetarse a las mismas.
- Informar a la Dirección Nacional de Tecnologia sobre cualquier situación anómala relacionada al certificado y que pueda resultar en la revocación de este.

11.12.7 EXENCIÓN DE RESPONSABILIDADES

La SAR-PKI solo responderá en el caso del no cumplimiento de las obligaciones contenidas en la Ley Sobre Firmas Electrónicas Decreto No. 149-2013, en la presente DPC y en las Políticas de Certificación especificas.

La SAR-PKI sólo responderá de los daños y perjuicios que en el ejercicio de su actividad ocasionen por la certificación u homologación de certificados de firmas electrónicas. En todo caso corresponde a SAR-PKI demostrar que actuó con la debida diligencia.

La SAR-PKI como Prestador de Servicios de Certificación, no se responsabiliza del contenido de los documentos firmados con sus certificados, ni de cualquier otro uso de sus certificados, como pueden ser procesos de cifrado de mensajes de datos o comunicaciones.

La SAR-PKI no representa en forma alguna a los usuarios ni a terceras partes aceptantes de los certificados que emite.

11.12.8 LIMITACIONES DE LAS RESPONSABILIDADES

La SAR-PKI no serán responsables de los daños y perjuicios ocasionados al firmante o terceros de buena fe, si el firmante incurre en alguno de los siguientes supuestos:

- No haber proporcionado a la SAR-PKI información veraz, completa y exacta sobre los datos que deban constar en el certificado electrónico o que sean necesarios para su expedición o para la extinción o suspensión de su vigencia, cuando su inexactitud no haya podido ser detectada por el prestador de servicios de certificación;
- La falta de comunicación sin demora a SAR-PKI de cualquier modificación de las circunstancias reflejadas en el certificado electrónico;
- Negligencia en la conservación de sus datos de creación de firma, en el aseguramiento de su confidencialidad y en la protección de todo acceso o revelación;
- No solicitar la revocación del certificado electrónico en caso de duda en cuanto al mantenimiento de la confidencialidad de sus datos de creación de firma;
- Utilizar los datos de creación de firma cuando haya expirado el periodo de validez del certificado electrónico o el prestador de servicios de certificación le notifique la extinción de su vigencia; y,
- Superar los límites que figuren en el certificado electrónico en cuanto a sus posibles usos y al importe individualizado de las transacciones que puedan realizarse con él o no utilizarlo conforme a las condiciones establecidas y comunicadas al firmante por la SAR-PKI.

La SAR-PKI tampoco serán responsables de los daños y perjuicios ocasionados al firmante o a terceros de buena fe, si el destinatario de los documentos firmados electrónicamente actúa de forma negligente.

Se entenderá, en particular, que el destinatario actúa de forma negligente en los casos siguientes:

- Cuando no compruebe y tenga en cuenta las restricciones que figuren en el certificado electrónico en cuanto a sus posibles usos y al importe individualizado de las transacciones que puedan realizarse con él; y,

- Cuando no tenga en cuenta la revocación o pérdida de vigencia del certificado electrónico publicada en el sitio web de SAR-PKI o cuando no verifique la firma electrónica.

La exención de responsabilidad frente a terceros obliga a la SAR-PKI a probar que actuó en todo caso con la debida diligencia.

11.12.9 **INDEMNIZACIONES**

El Servicio de Administración de Rentas responderá ante el Tribunal Contencioso Administrativo correspondiente por los daños y perjuicios que se cause al firmante, terceros o a cualquier persona, en el ejercicio de su actividad como prestador de servicios de certificación según lo estipulado en la Ley Sobre Firma Electrónica Decreto No. 149-2013, su reglamentación y la presente DPC. A tal efecto para el cálculo del monto de la indemnización se aplicarán las normas generales del procedimiento administrativo y responsabilidad contractual o extracontractual correspondientes.

11.12.10 **PERÍODO DE VALIDEZ**

11.12.10.1 **PERIODO**

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

Esta DPC se mantendrá vigente mientras se emita una nueva versión lo cual derogue expresamente la misma, o se haya realizado renovación de las claves de la Autoridad Certificadora de Honduras, momento en que obligatoriamente se dictará una nueva versión.

11.12.10.2 **TERMINACIÓN DE LA DPC**

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

Cuando la DPC quede derogada la misma deberá ser eliminada de los repositorios de SAR-PKI, si bien se conservará en archivo durante siete (7) años.

11.12.10.3 EFECTOS DE LA TERMINACIÓN

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

11.12.11 NOTIFICACIONES INDIVIDUALES Y COMUNICACIONES CON LOS PARTICIPANTES

Cualquier notificación, demanda, solicitud o cualquier otra comunicación requerida bajo las prácticas puntualizadas en esta DPC se realizará mediante mensaje electrónico o por escrito mediante correo certificado que tenga como remitente a cualquiera de las direcciones contenidas en el punto 6.4 Administración de las Políticas. Las comunicaciones electrónicas producirán sus efectos una vez que las reciba el destinatario al que van dirigidas.

11.12.12 ENMIENDAS

11.12.12.1 PROCEDIMIENTO PARA LAS ENMIENDAS

Tal cual se describe en las funciones de la Autoridad de Aprobación de Políticas, esta es la única entidad con la potestad para realizar y aprobar cambios sobre la DPC y las PC de la SAR-PKI.

11.12.13 RESOLUCIÓN DE CONFLICTOS

Todas reclamaciones entre usuarios y la PKI del Servicio de Administración de Rentas deberán ser notificadas por la parte en disputa a la Autoridad Administrativa Competente, Dirección Nacional de Tecnologia con el fin de expeditar la resolución entre las mismas partes.

En el caso de no alcanzar un acuerdo entre las partes, la resolución de cualquier disputa que pudiera surgir será supeditado, luego de agotada la via gubernativa al tribunal contencioso- administrativo correspondiente.

NORMATIVA APLICABLE

La totalidad de las normativas aplicables a las operaciones y funcionamiento de SAR-PKI, así como la presente Declaración de Prácticas de Certificación y las Políticas de Certificación estarán supeditadas a lo estipulado en la Ley Sobre Firma Electrónica Decreto No. 149-2013, publicado en la gaceta el 11 de diciembre del 2013 y sus reformas, su Reglamento y demás legislación aplicable.

11.12.15 CUMPLIMIENTO DE LA LEGISLACIÓN APLICABLE

Es obligación de la Autoridad Administrativa Competente asegurar el cumplimiento de la legislación aplicable recogida en el numeral anterior.

11.12.16 ESTIPULACIONES MISCELÁNEAS

11.12.16.1 ACEPTACIÓN DE LA DPC

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

11.12.16.2 RESOLUCIÓN DE CONFLICTOS JUDICIALMENTE

Los conflictos entre el Servicio de Administración de Rentas, suscriptores y terceros que se originen de la SAR-PKI como Prestador de Servicios de Certificación serán solventados, una vez agotada la vía gubernamental, ante el tribunal Contencioso-Administrativo correspondiente.

11.12.17 OTRAS ESTIPULACIONES

No se consideran otras estipulaciones.

12. GLOSARIO DE TÉRMINOS Y SIGLAS

12.1 DEFINICIONES

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

• **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.
• **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 si mismos y frente a terceros.
• **Persona Natural:**	Individuo debidamente identificado en el territorio de la República de Honduras, mediante su Tarjeta de Identidad.
• **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 SAR-PKI.
- **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 Dirección Nacional de Tecnologia.
- **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.

12.2 ACRÓNIMOS

- **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:**	Politica 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.
• **SAR-PKI:**	Infraestructura de Clave Pública del Servicio de Administración de Rentas.
• **ST:**	State - Estado. Correspondiente a estándar x.500.