POLÍTICA

DE CERTIFICADO DE FIRMA ELECTRÓNICA AVANZADA DE EMPLEADO(A) PÚBLICO(A)

POL-GIF-GGI-NDP-020-V2

SAR

SERVICIO DE ADMINISTRACIÓN DE RENTAS

DIRECCIÓN EJECUTIVA

SECRETARÍA GENERAL

Febrero 2023

FECHA VIGENCIA: Febrero 2023	CÓDIGO: POL-GIF-GGI-NDP-020-V1	VERSIÓN 2	N° PÁGINAS 69

POLÍTICA DE CERTIFICACIÓN DE CERTIFICADO DE FIRMA ELECTRÓNICA AVANZADA DE EMPLEADO(A) PÚBLICO(A)

RUBRO	CARGO	FIRMA
APROBADO POR:	Lic. Marlon David Ochoa Martínez **Director Ejecutivo**	
	Lic. Christian David Duarte Chávez **Sub-Director Ejecutivo**	
	Lic. Alessandra Vanesa Díaz Tovar **Directora Nacional de Gestión Estratégica**	
	Abg. Gersson Orlando Sierra Portillo **Director Nacional Jurídica**	
	Ing. Diana Orestila Cárcamo Rodríguez **Directora Nacional de Tecnología**	
	Abg. Nidia Sarahí Berrios Martínez **Secretaria General**	
	Abg. Celvin Antonio Ruíz Lobo **Inspector General**	

REVISADO POR:	Mayda Arely Sosa Alvarez **Experta Departamento de Procuración Legal**	
	Abg. Fátima Isabel Estrada Saravia **Experta Departamento de Asesoría Legal**	
	Abg. Carlos Antonio García García **Especialista de Secretaría General**	
ELABORADO POR:	Ing. Osman René Moreno Ramos **Experto Dirección Nacional de Tecnología**	
	Lic. Antonio Bustillo Banegas **Analista de Innovación y Mejora Continua**	

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 son 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.

Contenido

1. INTRODUCCIÓN

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

Con el propósito de facilitar la lectura y análisis del documento, se incluyen todas las secciones establecidas en dicha RFC apareciendo la frase "No estipulado" en las secciones para las que no se haya previsto nada.

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

El presente documento es de carácter público y se encuentra dirigido a todas las personas naturales y jurídicas, empleados(as) públicos(as), y terceros que confían en los certificados y servicios de sellado de tiempo brindados por el SAR.

1.1. VISIÓN GENERAL

1.1.1. CONTROL DE DOCUMENTOS

Versión	Motivo	Fecha de vigencia	Documentos que elimina
1.0	Creación	Diciembre 2021	N/A
2.0	Actualización	Febrero 2023	ACUERDO número- SAR-521 -2021, Manual de Procedimiento de Firma Electrónica Avanzada de Funcionario Público, MPR-GIT-TIG-AEB-003-V1

1.1.2. OBJETIVO ESTRATÉGICO VINCULADO AL DOCUMENTO

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

1.1.3. DOCUMENTO RELACIONADO

Nombre del Documento Relacionado	Código o número de acuerdo o del Documento Relacionado
Estatuto Orgánico	Acuerdo Número SAR-109-2019
Política Declaración de Prácticas de Certificación de Infraestructura de Clave Pública del Servicio de Administración de Rentas de la República de Honduras	Acuerdo Número SAR-057-2023

1.1.4. IDENTIFICACIÓN DEL PROCESO

MACROPROCESO:	4.Gestión de la Información
PROCESO A PRIMER NIVEL:	4.1. Gestión del Gobierno de la Información
VERSIÓN DEL DOCUMENTO:	2
RESPONSABLE DEL PROCESO:	Secretaría General

1.1.5. OBJETIVO

El presente documento contiene las Políticas de Certificación de Certificado de Firma Electrónica Avanzada de Empleados(as) Públicos(as), las cuales rigen el funcionamiento y operaciones de la Infraestructura de Clave Pública de Servicio de Administración de Rentas (PKI-SAR).

1.1.6. ALCANCE

La totalidad de los Certificados de Firma Electrónica Avanzada de Empleado(a) Público(a), emitidos por la PKI del Servicio de Administración de Rentas de Honduras, cumplen con lo estipulado en estándar RFC 3647 "Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework". De esta manera se hace posible la adición de extensiones para la certificación de atributos.

El alcance del presente documento se encuentra dirigido a todas las personas naturales y jurídicas, empleados(as) públicos(as), y terceros que confían en los certificados y servicios de sellado de tiempo brindados por el SAR.

1.1.7. NORMAS Y DISPOSICIONES

a. Lo establecido en este documento es de aplicación para los Suscriptores de certificado electrónico emitidos por el Servicio de Administración de Rentas así como los terceros que confían en la emisión de los certificados por el PKI-SAR.

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

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

d. Esta PC establece los requisitos particulares emitidos por Thomas Signe S.A.S, siguiendo el estándar RFC 3647 "Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework", y conforme a los estándares descritos en el numeral 1.1.9 Referencia técnica.

1.1.8. EXCLUSIONES

Este documento ha sido diseñado basado en las recomendaciones de la RFC 7382 (Plantilla Para una Declaración de Prácticas de Certificación (CPS) para la PKI de recursos (RPKI)), con la finalidad de hacer de fácil comprensión para el lector. Existen secciones las cuales se determina como "No Estipulado", dichas secciones del documento no tienen inherencia en nuestro marco de cumplimiento.

1.1.9. MARCO NORMATIVO

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

1.1.10. REFERENCIA TÉCNICA

Documentos de Referencia	Fecha de vigencia
Recomendaciones del RFC 2560	1999
Recomendaciones del RFC 3161 – TSA	2001
Recomendaciones del RFC 5280 – CRL	2008
Recomendaciones del RFC 6960 – OSCP	2013
ISO/IEC 27001 – Sistema de gestión de seguridad	2018
ISO/IEC 27001 – Sistema de gestión de seguridad	2018

1.2. NOMBRE DEL DOCUMENTO E IDENTIFICACIÓN DE LA PC

El nombre de este documento es "Política de Certificación de Certificado de Firma Electrónica Avanzada de Empleado(a) Público(o), versión 2", la cual entra en vigencia a partir de la fecha de su publicación, y debe de ser sustituida al momento de la elaboración y publicación de una nueva versión.

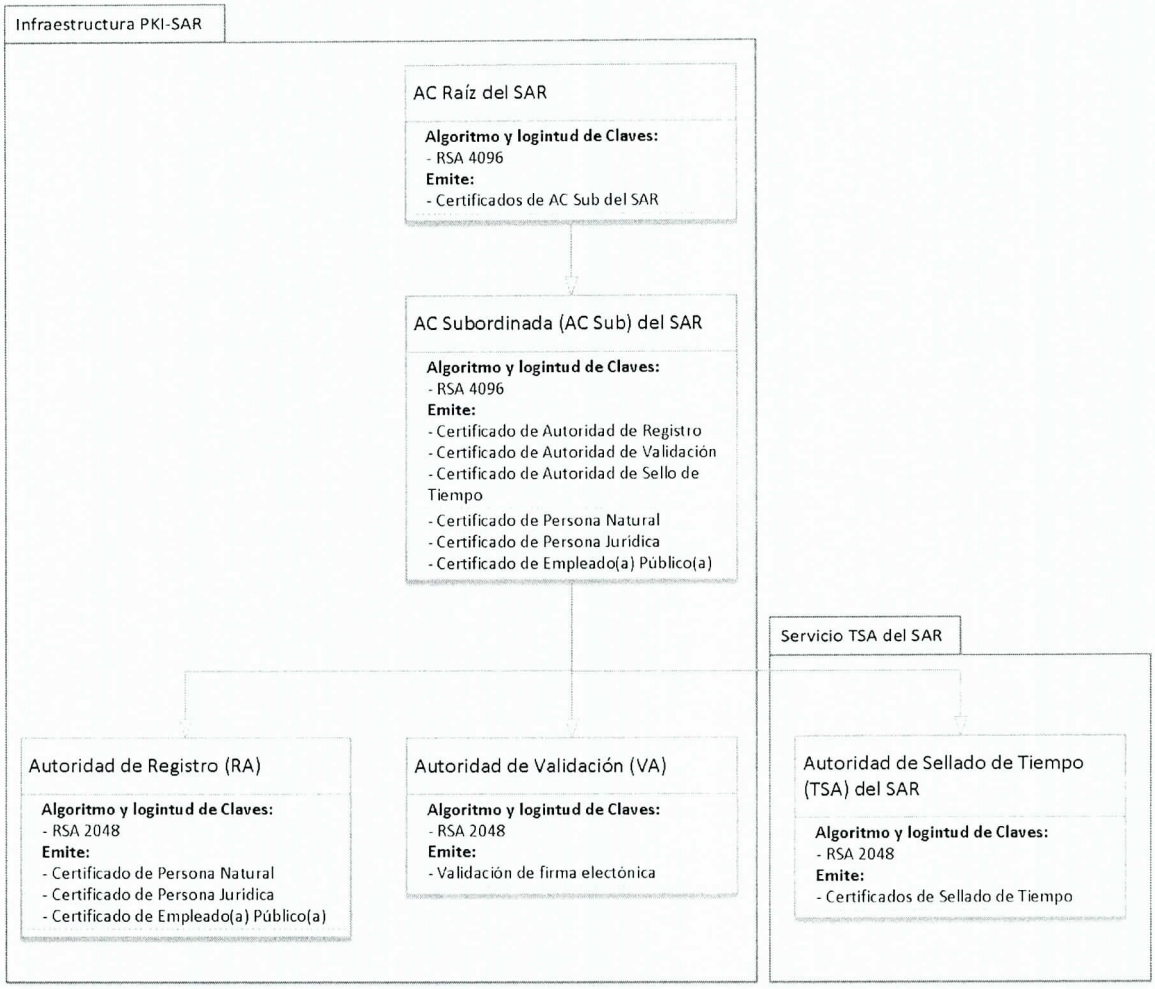
El URL para acceder públicamente a este documento se encuentra en la dirección https://www.sar.gob.hn/firmaelectronica/ Y el Identificador de Objetos (OID) correspondiente a este documento es el 1.3.6.1.4.1.52089.2.4

1.3. PARTICIPANTES DE LA PKI-SAR

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

- Autoridad de Certificación (AC).
- Autoridad de Registro (AR).
- Autoridad de Validación (AV).
- Autoridad de Sellado de Tiempo (AST).
- Comité de Firma Electrónica.
- Solicitantes y Suscriptores de certificados
- Terceros que confían en los certificados de la PKI del Servicio de Administración de Rentas.
- Autoridad Administrativa Competente (AAC).
- Prestador de Servicios de Certificación (PSC).

Para tener una visión clara de toda la jerarquía de confianza de la PKI-SAR, se presenta la siguiente infraestructura:



1.3.1. AUTORIDADES DE CERTIFICACIÓN (AC)

Podrán actuar como Autoridad Certificación, las personas naturales, y las personas jurídicas, tanto públicas como privadas, que sean autorizadas por la Autoridad Administrativa Competente (AAC), para operar como tales y que cumplan con los requerimientos establecidos en la Ley, sobre Firmas Electrónicas y su Reglamento, la Infraestructura Oficial de la Firma Electrónica y por la misma Autoridad Administrativa Competente (AAC).

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

1.3.2. AUTORIDAD CERTIFICADORA RAÍZ DEL SAR

La PKI-SAR es la designada para realizar la emisión de los certificados, los cuales son objeto de la presente PC es regida bajo el Certificado Raíz, el que consiste en un certificado autofirmado con el cual se inicia 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.

Contenido del certificado Autoridad Certificadora Raíz del SAR				
Nombre	**Atributo**	**Valor**	**Obligatorio**	**Crítica**
Version	-	3	Si	-
Serial Number	-	2B C0 4A F2 74 CA 86 9B 11 33 95 4E F8 27 92 0F CB E8 BD CF	Si	-
Signature	Algorithm	Sha256WithRSAEncryption	Si	-
Issuer	CN	AUTORIDAD CERTIFICADORA RAIZ DEL SAR	Si	-
	O	SERVICIO DE ADMINISTRACIÓN DE RENTAS	Si	-
	C	HN	Si	-
Validity	Not After	2023-02-28 12:25:02	Si	-
	Not Before	2043-02-28 12:25:20	Si	-
Subject	CN	AUTORIDAD CERTIFICADORA RAIZ DEL SAR	Si	-
	O	SERVICIO DE ADMINISTRACIÓN DE RENTAS	Si	-
	C	HN	Si	-
Subject Public Key Info	Algorithm	RSA	Si	-

1.3.3. AUTORIDAD CERTIFICADORA SUBORDINADA DEL SAR

La PKI-SAR implementa una AC subordinada. Dicha AC es la siguiente en jerarquía a la ACR; por lo tanto, la Autoridad Certificadora Subordina es la encargada de la emisión de todos los certificados de persona natural, persona jurídica y empleados(as) públicos(as).

En la siguiente tabla se detallan los datos con más relevancia de la Autoridad Certificadora del SAR.

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

1.3.4. AUTORIDAD DE REGISTRO (AR)

La Autoridad de Registro (AR) es la responsable de la gestión de las solicitudes, identificación, registro y aprobación de los certificados emitidos por la PKI-SAR y cualquier responsabilidad específica establecida en la DPC y cada una de las PC. Asimismo, es la entidad encargada de:

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

1.3.5. AUTORIDAD DE VALIDACIÓN (AV)

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

El mecanismo antes mencionado, es complementario al proceso de publicación de las Listas de Certificados Revocados (CRL).

1.3.6. AUTORIDAD DE SELLADO DE TIEMPO (AST)

La Autoridad de Sellado de Tiempo (AST) es la responsable de probar que un conjunto de datos que existió antes de un momento dado y que, ninguno de estos datos, ha sido modificado desde entonces de acuerdo con el estándar RFC 3161.

1.3.7. SOLICITANTES Y SUSCRIPTORES DE CERTIFICADOS

Los Solicitantes y Suscriptores de certificados son definidos por la DPC de la PKI-SAR. Dentro del contexto de esta PC, los Suscriptores y Solicitantes de "Certificado de Firma Electrónica" es cualquier persona natural que posea documento Nacional de Identificación (DNI) de Honduras o una persona extranjera residente en

Honduras que presente su carnet de residencia, un extranjero no residente con su pasaporte vigente y empleados(as) públicos(as) con la documentación que acredite que ostentan un cargo en la Administración Pública.

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

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

1.3.9. AUTORIDAD ADMINISTRATIVA COMPETENTE (AAC)

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

1.3.10. PRESTADOR DE SERVICIOS DE CERTIFICACIÓN (PSC)

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

- Emitir certificados en relación con las firmas electrónicas certificadas de empleado(a) público(a), persona natural y persona jurídica.
- Emitir certificados sobre la verificación respecto de la alteración entre el envío y recepción del mensaje de datos.
- Ofrecer o facilitar los servicios de creación de firma electrónica avanzada;
- Ofrecer o facilitar los servicios de registro y estampado cronológico en la generación, transmisión y recepción de mensajes de datos.
- Ofrecer los servicios de archivo y conservación de mensajes de datos.

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

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

Para verificar que las AC o PSC cumplan con los requerimientos antes establecidos y determinar el grado de fiabilidad de dichos prestadores, se toman 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 debe ser competente para las funciones que realiza, quienes estarán encargados de la emisión de opiniones técnicas que se requieran, la formulación de políticas y su implementación.
- Experiencia en tecnologías de clave pública y familiaridad con procedimientos de seguridad apropiados.
- Contar con el equipo y los programas informáticos necesarios.

- Mantenimiento de un registro de auditoría y realización de auditorías por una Autoridad independiente.
- Existencia de un plan para casos de emergencia (por ejemplo, "programas de recuperación en casos de desastre" o depósitos de claves).
- Disposiciones para proteger su propia clave privada.
- Seguridad interna.
- Disposiciones para suspender las operaciones, incluida la notificación a los usuarios.
- Declaración de limitación de la responsabilidad.
- Contar con procedimientos de revocación (en caso de que la clave criptográfica se haya perdido o haya quedado en entredicho).

1.4. USO DE LOS CERTIFICADOS

1.4.1. USO ADECUADO DE LOS CERTIFICADOS

El uso adecuado de los certificados descritos en esta PC es para la firma realizada por los empleados(as) públicos(as), con cargos en la entidad pública Suscriptora, de acuerdo con su cargo, empleo y/ o en su caso, condición de autorización.

El SAR y la entidad pública Suscriptora, pueden fijar en los convenios y acuerdos, a través del documento de relación correspondiente, otros límites y la forma de comunicaciones a través de medios electrónicos, informáticos y telemáticos para realizar las respectivas validaciones.

1.4.2. PROHIBICIONES DE USO DE LOS CERTIFICADOS

Los certificados de empleado(a) público(a) no deben emplearse para ninguna propósito que no esté especificado en el numeral 1.4.1. uso adecuado de los certificados.

1.5. ADMINISTRACIÓN DE LAS POLÍTICAS

1.5.1. ORGANIZACIÓN RESPONSABLE DE ADECUACIÓN DE LAS POLÍTICAS

Los términos y redacción de la presente Política de Certificación de Empleado(a) Público(a) son establecidos por el Servicio de Administración de Rentas a través de su Comité de Firma Electrónica; quien es el responsable también de realizar las revisiones periódicas de las mismas, de manera que se mantengan actualizadas.

1.5.2. PROCEDIMIENTO DE APROBACIÓN Y MODIFICACIÓN DE LA POLÍTICA DE CERTIFICACIÓN DE EMPLEADOS(AS) PÚBLICOS(AS)

El SAR, a través de su Comité de Firma Electrónica, vela por el cumplimiento de la Política de Certificación de Empleados(as) Públicos(as), así como el pertinente proceso de revisión y aprobación de esta.

1.5.3. RESPONSABLE POR MODIFICACIONES A LA PC

La responsabilidad de las aprobaciones y modificaciones correspondientes de la PC corresponde de manera exclusiva al Comite 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 PC son publicadas en el sitio web de Servicio de Administración de Rentas, en la dirección https://sar.gob.hn/firmaelectronica/. 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 le da derecho al Suscriptor de recibir compensación por este motivo.

1.5.4. DATOS DE CONTACTO

Nombre de Entidad: Servicio de Administración de Rentas - SAR

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

Correo: pki@sar.gob.hn

Teléfono: (504) 2216-5800

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

1.6. GLOSARIO Y ABREVIATURAS

1.6.1. GLOSARIO

- **Autenticación:** Proceso de intento de verificar la identidad digital de los Solicitantes o Suscriptores de un certificado de la República de Honduras, de este modo la PKI-SAR se asegura de que los Solicitantes o Suscriptores son quien ellos dicen ser.

- **Autoridad:** Entidad dentro de la PKI con tareas específicas de acuerdo con su rol como certificador, validador o registro.

- **Certificado Electrónico:** Todo mensaje de datos proporcionado por un "Prestador de servicios de certificación" que le atribuye certeza y validez a la firma electrónica.

- **Clave Privada:** Componente confidencial del Suscriptor, utilizado para el proceso de cifrado o firmado electrónico.

- **Clave Pública:** Componente de carácter público que corresponde a una clave privada, utilizado para el descifrado de información o verificación de identidad de firmas electrónicas.

- **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.

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

- **Interoperabilidad:** Es la capacidad y procedimientos, de compartir datos y posibilitar el intercambio de información con terceros.

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

- **Oficina de Registro:** Lugar designado por la PKI-SAR para la generación del Certificado De Empleado(a) Público(A), previa validación del proceso de generación de este.

- **Persona Jurídica:** Entidad debidamente registrada en el territorio hondureño, con capacidad suficiente para contraer obligaciones y realizar actividades que generan plena responsabilidad jurídica, frente a sí mismos y frente a terceros.

- **Persona Natural:** Individuo debidamente identificado en el territorio de la República de Honduras, mediante Documento Nacional de Identificación.

• **Prestador de Servicios de Certificación:**	Un prestador de servicios de certificación es una persona, física o jurídica, que expide certificados electrónicos o que presta otros servicios en relación con la firma electrónica.
• **Repositorio Criptográfico de Software PKCS12:**	Archivo para el almacenamiento de muchos objetos criptográficos en un solo archivo.
• **Repositorios:**	Archivo en 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.
• **Signos distintivos:**	Son todos aquellos símbolos, figuras, vocablos o expresiones que se utilizan en la industria o en el comercio para distinguir un producto, servicio o establecimiento.
• **Solicitante:**	Individuo que solicita un certificado electrónico mediante los procesos provistos por la PKI-SAR.
• **Suscriptor:**	Entidad final para quien se han emitido certificados.
• **Tercero que confía:**	Individuo o entidad distinta del Suscriptor que decide confiar en los

certificados electrónicos emitidos por PKI-SAR.

- **Unicidad:** Calidad de único o el hecho de las propiedades de cierto objeto definido hace que éste sea único.

- **Validación:** Proceso mediante el cual se verifica la certeza de los datos provistos por el Solicitante. En el caso de certificados, corresponde a la verificación del estado de estos.

1.6.2. SIGLAS

- **AAC:** Autoridad Administrativa Competente.
- **AC:** Autoridad de Certificación.
- **AR:** Autoridad de Registro.
- **AV:** Autoridad de Validación.
- **C:** Country (País). Correspondiente a estándar x.500.
- **CDP:** CRL Distribution Point - Punto de Distribución de CRL.
- **CN:** Common Name - Nombre Común. Correspondiente a estándar x.500.
- **CRL:** Certificate Revocation List - Lista de Revocación de Certificados.
- **DN:** Distinguished Name - Nombre Distintivo. Correspondiente a estándar x.500.
- **DPC:** Declaración de Practicas de Certificación.
- **FIPS:** Federal Information Processing Standard-stándares federales de procesamiento de la información.
- **HSM:** Hardware Security Module. Componente informático de hardware que salvaguarda y gestiona claves electrónicas.
- **L:** Localidad o Dirección. Correspondiente a estándar x.500.
- **O:** Organization - Organización. Correspondiente a estándar x.500.

- **OCSP:** Online Certificate Status Protocol. Método para determinar el estado de vigencia de un certificado digital X.509.
- **OID:** Object Identifier - Identificador Único de Objeto.
- **OU:** Organizational Unit - Unidad Organizacional. Correspondiente a estándar x.500.
- **PC:** Política de Certificación.
- **PIN:** Personal Identificacion Number – Contraseña que protege el acceso a datos.
- **PKCS:** Public Key Cryptography Standards. Estandar Internacional.
- **PKI:** Public Key Infrastructure - Infraestructura de Clave Pública.
- **PSC:** Proveedor de Servicios de Certificación.
- **RFC:** Request For Comments. Estandar desarrollado por el Internet Engineering Task Force.
- **PKI-SAR:** Infraestructura de Clave Pública del Servicio de Administración de Rentas.
- **ST:** State - Estado. Correspondiente a estándar x.500.

2. REPOSITORIOS Y PUBLICACIÓN DE INFORMACIÓN

2.1. REPOSITORIOS

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

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

2.2. PUBLICACIÓN DE INFORMACIÓN DE CERTIFICACIÓN

La Política de Certificación de Empleado(a) Público(a) es de carácter público y se encuentra publicada en el sitio web de PKI-SAR, al que se hace mención en el numeral 2.1. Repositorios.

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

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

2.3. TIEMPOS Y FRECUENCIA DE PUBLICACIÓN

La Política de Certificación de Empleado(a) Público(a) es publicada consecuentemente al momento de su aprobación. Dicha documentación es publicada en el sitio web al que se hace mención en el numeral 2.1. Repositorios.

La AC debe agregar los certificados que son revocados a la CRL correspondiente, la ventana de tiempo es acorde al punto 4.9.7. Frecuencia de emisión de CRL.

2.4. CONTROLES DE ACCESO A LOS REPOSITORIOS

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

3. IDENTIFICACIÓN Y AUTENTICACIÓN

3.1. NOMBRES

3.1.1. TIPOS DE NOMBRES

La totalidad de los Suscriptores de certificados requieren de un Distinguished Name, el cual debe cumplir con el estándar RFC 5280 "Internet X.509 Publick Key Infraestructure Certificate and Certificate Revocation List (CRL)".

A continuación, se define el procedimiento de asignación de los nombres distintivos para los Certificados de Empleado(a) Público(a).

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

3.1.2. NECESIDAD DE QUE LOS NOMBRES SEAN SIGNIFICATIVOS

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

3.1.3. REGLA PARA INTERPRETAR VARIOS FORMATOS DE NOMBRES

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

3.1.4. UNICIDAD DE LOS NOMBRES

La agrupación del Nombre Distintivo (DN), más el contenido de la extensión Policy Indentifier, es único y no confuso. El uso del número de identidad o pasaporte en el campo Nombre Común (CN) garantiza la unicidad de este.

3.1.5. RECONOCIMIENTO, AUTENTICACIÓN Y PAPEL DE LAS MARCAS REGISTRADAS

El SAR no asume compromiso alguno sobre el uso de marcas comerciales o signos distintivos, registrados o no, en la emisión de los certificados expedidos. Solo se permite la solicitud de certificados que incluyan signos distintivos cuyo derecho de uso sea propiedad del Titular o se encuentre debidamente autorizado. El SAR no está obligado a verificar previamente la titularidad o registro de los signos distintivos antes de la emisión de los certificados, aunque figuren en registros públicos.

3.2. VALIDACIÓN INICIAL DE IDENTIDAD

3.2.1. MÉTODOS PARA COMPROBAR LA CLAVE PRIVADA

El SAR no genera, ni almacena, las claves privadas asociadas a los Certificados De Empleado(a) Público(a), expedidos bajo las presentes Políticas de Certificación. Las claves privadas son generadas bajo el exclusivo control del firmante, con la intervención de la Oficina de Registro correspondiente, y cuya custodia está bajo responsabilidad del titular del certificado.

Para la expedición de los Certificados de Empleado(a) Público(a), se requiere que el Solicitante genere la clave privada en el sistema del PKI-SAR después de haber sido registrado y una vez validada dicha generación por parte de la Oficina de Registro, tras el proceso de acreditación de la identidad del citado Solicitante y recabada su voluntad.

3.2.2. AUTENTICACIÓN DE LA IDENTIDAD DE LA ORGANIZACIÓN

Con carácter previo al establecimiento de cualquier relación institucional con los Suscriptores, la PKI-SAR valida las condiciones del servicio, así como de las obligaciones, garantías y responsabilidades de las partes implicadas en la expedición y uso de los Certificado de Empleado(a) Público(a).

3.2.3. AUTENTICACIÓN DE LA IDENTIDAD DE LA PERSONA FÍSICA SOLICITANTE

Es responsabilidad de cada entidad pública del Estado de Honduras, verificar que el empleado solicitante de certificado cuente con su cargo vigente, tenga su número de identificación personal, que su empleo o autorización es auténtico y está en vigor; y, por lo tanto, esté habilitado para obtener y usar los Certificados de Firma Electrónica de Empleado(a) Público(a).

El SAR no ostenta relación jurídica, funcional, administrativa o laboral con tal personal, más allá del documento de aceptación de condiciones del uso del Certificado de Empleado(a) Público(a).

La validación de los datos del perfil depende del convenio que se suscribe con la entidad a la que pertenezca el/la empleado(a) público(a).

3.2.4. INFORMACIÓN NO VERIFICADA SOBRE EL SOLICITANTE

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

3.2.5. COMPROBACIÓN DE LAS FACULTADES DE REPRESENTACIÓN

Este punto no es aplicable ya que para poder autenticar la identidad de un empleado(a) público(a), este debe comparecer personalmente a la Oficina de Registro con su Documento Nacional de Identificación, Carnet de Residencia o Pasaporte Vigente.

3.2.6. CRITERIOS PARA INTEROPERABILIDAD

Como establezca la DPC de la PKI-SAR, en el numeral 3.2.6 Criterios para Interoperabilidad.

3.3. IDENTIFICACIÓN Y AUTENTICACIÓN PARA SOLICITUDES DE RENOVACIÓN DE CLAVES

La Política de Certificación de Empleado(a) Público(a) no contempla ningún proceso de regeneración de claves.

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

3.4. IDENTIFICACIÓN Y AUTENTICACIÓN PARA SOLICITUDES DE REVOCACIÓN

Previo a la revocación efectiva de los certificados, la persona asignada en la Oficina de Registro identifica de forma fehaciente al Solicitante de la revocación para vincularlo, con los datos únicos del certificado de revocación.

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

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

4.1. SOLICITUD DE CERTIFICADOS

4.1.1. QUIEN PUEDE REALIZAR UNA SOLICITUD

La solicitud de Certificado de Empleado(a) Público(a) es efectuada por las personas designadas por la institución pública para realizar este trámite con el SAR, posterior al convenio firmado para las condiciones de uso de los Certificados de Empleado(a) Público(a).

4.1.2. PROCESO DE ENROLAMIENTO Y RESPONSABILIDADES DE LOS SOLICITANTES

El/la Empleado(a) Público(a) quien es el titular asignado para obtener un certificado, debe solicitar una cita a través de la aplicación KIIN en la dirección suscrita en la página web https://www.sar.gob.hn/kiin/.

El día de la cita, el Solicitante se presenta a la Oficina de Registro seleccionada en dicha aplicación, identificándose con el Documento Nacional de Identificación personal. Adicionalmente, es necesario la presentación del documento que sustenta su condición de servidor público. Una vez verificada la documentación y su autorización conforme al listado emitido con la entidad con la cual se suscribió el convenio, se procede a realizar el ingreso de los datos personales y laborales en el sistema del PKI-SAR, así como la emisión del certificado.

Es responsabilidad del Solicitante del certificado garantizar la completitud y veracidad de toda la información aportada para obtener su Certificado de Empleado(a) Público(a); lo anterior, sin menoscabo de las comprobaciones realizadas por la Oficina de Registro.

4.2. GESTIÓN DE LAS SOLICITUDES DE CERTIFICADOS

4.2.1. FUNCIONES DE IDENTIFICACIÓN Y AUTENTICACIÓN

Para el Certificado de Empleado(a) Público(a), el Solicitante aporta los datos requeridos, acredita su Documento Nacional de Identificación personal y su condición de empleado(a) público(a). El personal asignado a la Oficina de Registro constata la identidad del Solicitante y conserva la documentación que la acredite.

4.2.2. RECHAZO O ACEPTACIÓN DE SOLICITUDES DE CERTIFICADO

El Certificado de Empleado(a) Público(a), una vez confirmada la identidad del Solicitante y la vigencia del cargo, el personal asignado por la Oficina de Registro, procede a enviar el certificado por medio de correo electrónico.

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

- Documento de identificación no es válido.
- El Solicitante no tiene autorización para solicitar la emisión de certificado (como se defina en el convenio establecido con el SAR).
- Si la información concerniente a identificación y autenticación de toda la información requerida en cada PC no está completa.
- La inexistencia de registro de datos en la Institución a la que el empleado(a) público(a) pertenece o los datos que no son consistentes con la forma de solicitud de certificación.
- Otras, dependiendo de la particularidad de la documentación solicitada para cada tipo de certificado, las que se estipulan en cada una de las políticas de certificación correspondientes.

4.2.3. PLAZO PARA LA GESTIÓN DE LAS SOLICITUDES

La AC de la PKI-SAR no es responsable por el retraso que pueda surgir entre la solicitud del certificado y la entrega de este. En cualquier caso, el plazo para la tramitación de las solicitudes de certificados está condicionada a la disponibilidad

de citas en las Oficinas de Registro, a la que desee acudir el Solicitante; y, de igual manera, a la carga administrativa interna de la AC.

4.3. EMISIÓN DE CERTIFICADOS

4.3.1. ACCIONES DE LA AC DURANTE LA EMISIÓN DE CERTIFICADO

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

La vigencia del certificado inicia al momento de emisión de este. El periodo de validez o vigencia del certificado puede estar sujeto de una expiración anticipada, temporal o definitiva: esto en el caso de que se den las causas necesarias que motiven a la suspensión o revocación de este.

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

Una vez emitido el Certificado de Empleado(a) Público(a), la PKI-SAR informa por medio de correo electrónico al Solicitante sobre la disponibilidad del certificado para su descarga.

4.4. ACEPTACIÓN DEL CERTIFICADO

4.4.1. ACCIÓN QUE AFIRMA LA ACEPTACIÓN DEL CERTIFICADO

En el proceso de solicitud del Certificado de Empleado(a) Público(a), el Solicitante acepta las condiciones de uso y expresa su voluntad de obtener el certificado como requisitos necesarios para la generación de este.

4.4.2. PUBLICACIÓN DEL CERTIFICADO POR PARTE DE LA AC

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

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

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

4.5. USO DEL PAR DE CLAVES Y CERTIFICADO

El Certificado de Empleado(a) Públicos(a) es de uso intransferible, mismo que acredita la identidad de su titular, así como su cargo en la administración pública. Su emisión es para el uso exclusivo en el ámbito de sus funciones de forma personalísima e indelegable.

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

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

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

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

Los terceros que confían sólo pueden depositar su confianza en los certificados para el uso exclusivo en el ámbito de sus funciones en el cargo de la administración pública y de acuerdo con lo establecido en el campo 'Key Usage' y 'Extended Key Usage' del certificado.

Es responsabilidad de los terceros que confían el realizar la operación de clave pública siguiendo el procedimiento adecuado para confiar en el certificado, así como también realizar la verificación del estado de certificado utilizando el medio establecido en la DPC y la presente PC.

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

4.6. RENOVACIÓN DE CERTIFICADOS SIN CAMBIO DE CLAVE

4.6.1. CIRCUNSTANCIAS PARA LA RENOVACIÓN DE CERTIFICADOS SIN CAMBIO DE CLAVE

Bajo la presente PC, la PKI-SAR no renueva certificado sin cambio de clave. Por lo tanto, los numerales siguientes referentes a la renovación de certificados sin cambios de clave (puntos 4.6.2, 4.6.4, 4.6.5, 4.6.6, 4.6.7 y 4.6.7), se consideran como no estipulados en este documento.

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

No estipulado.

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

No estipulado.

4.6.4. NOTIFICACIÓN DE LA EMISIÓN DE UN NUEVO CERTIFICADO AL SUSCRIPTOR

No estipulado.

4.6.5. FORMA DE ACEPTACIÓN DEL CERTIFICADO SIN CAMBIO DE CLAVE

No estipulado.

4.6.6. PUBLICACIÓN DEL CERTIFICADO SIN CAMBIO DE CLAVE

No estipulado.

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

No estipulado.

4.7. RENOVACIÓN DE CERTIFICADOS CON CAMBIO DE CLAVES

Bajo la presente Política de Certificación, la renovación con regeneración de clave del Certificado de Empleado(a) Público(a) se realiza siempre emitiendo nueva clave, siguiendo el mismo proceso que está descrito en la emisión de un certificado nuevo; por ello, se debe remitir a dicho apartado.

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

No estipulado.

4.7.2. QUIÉN PUEDE PEDIR LA RENOVACIÓN DE LOS CERTIFICADOS

Se sigue el mismo proceso que esta descrito en la emisión de un certificado nuevo.

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

Se sigue el mismo proceso que esta descrito en la emisión de un certificado nuevo.

4.7.4. NOTIFICACIÓN DE LA EMISIÓN DE UN NUEVO CERTIFICADO AL SUSCRIPTOR

Se sigue el mismo proceso que esta descrito en la emisión de un certificado nuevo.

4.7.5. MÉTODO DE ACEPTACIÓN DEL CERTIFICADO CON CAMBIO DE CLAVES

Se sigue el mismo proceso que esta descrito en la emisión de un certificado nuevo.

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

Se sigue el mismo proceso que esta descrito en la emisión de un certificado nuevo.

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

Se sigue el mismo proceso que esta descrito en la emisión de un certificado nuevo.

4.8. MODIFICACIÓN DE CERTIFICADOS

No es posible realizar modificaciones al Certificado de Empleado(a) Público(a) expedido. Por tanto, cualquier necesidad de modificación conlleva a la expedición de un nuevo certificado. Consecuentemente, el resto de los incisos siguientes referentes a la modificación de certificados (puntos 4.8.1, 4.8.2, 4.8.3, 4.8.4, 4.8.5, 4.8.6, 4.8.7) se consideran como no estipulado en este documento.

4.8.1. CIRCUNSTANCIAS PARA LA MODIFICACIÓN DEL CERTIFICADO

No estipulado.

4.8.2. QUIÉN PUEDE SOLICITAR LA MODIFICACIÓN DE LOS CERTIFICADOS

No estipulado.

4.8.3. GESTIÓN DE LAS PETICIONES DE MODIFICACIÓN DE CERTIFICADOS

No estipulado.

4.8.4. NOTIFICACIÓN POR LA EMISIÓN DE UN CERTIFICADO MODIFICADO AL SUSCRIPTOR

No estipulado.

4.8.5. MÉTODO DE ACEPTACIÓN DEL CERTIFICADO MODIFICADO

No estipulado.

4.8.6. PUBLICACIÓN DEL CERTIFICADO MODIFICADO POR LA AC

No estipulado.

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

No estipulado.

4.9. REVOCACIÓN Y SUSPENSIÓN DE CERTIFICADOS

4.9.1. CIRCUNSTANCIAS PARA LA REVOCACIÓN

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

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

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

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

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

4.9.2. QUIÉN PUEDE SOLICITAR LA REVOCACIÓN

La revocación de un Certificado de Empleado(a) Público(a) solamente puede ser solicitado por:

- La autoridad judicial.

- El Suscriptor o un tercero en su nombre y representación, debidamente facultado.

La AC de la PKI-SAR puede revocar de oficio el Certificado de Empleado(a) Público(a) si tuviera conocimiento o sospecha del compromiso de la clave privada del titular o cualquier otro hecho recogido en la presente PC.

4.9.3. PROCEDIMIENTO DE SOLICITUD DE REVOCACIÓN

La solicitud de revocación de Certificado de Empleado(a) Público(a) la efectúa la institución pública a la cual pertenece el/la empleado(a), a través de la Oficina de Talento Humano o la oficina que se designe como enlace en el convenio establecido con el SAR. Para ello, se debe presentar la documentación que acredite la solicitud de revocación: resolución administrativa, acuerdo de cancelación o renuncia, acta de defunción o cualquier otro documento que sustente el cese definitivo del certificado electrónico.

De igual forma, el Suscriptor del Certificado puede solicitar la revocación en el caso de verse comprometidas las claves o por errores contenidos en el certificado.

Una vez que la PKI-SAR ha procedido a la revocación del Certificado de Empleado(a) Público(a), se publica en el directorio seguro, la correspondiente Lista de Certificados Revocados, conteniendo el número de serie del Certificado Revocado, así como la fecha y hora. Una vez que un certificado ha sido revocado, su vigencia queda definitivamente extinguida, sin posibilidad de revertir su estado.

4.9.4. PERIÏODO EN QUE DEBE PROCESAR LAS SOLICITUDES DE REVOCACIÓN

No existe periodo de gracia para este proceso, debido a que la revocación es ejecutada de manera inmediata a la tramitación de la solicitud que sea verificada como válida.

4.9.5. PLAZO EN EL QUE DEBE RESOLVER LA SOLICITUD DE REVOCACIÓN

La PKI-SAR procede a la revocación inmediata del certificado en el momento de verificar la identidad del Solicitante o, la veracidad de la solicitud que se realiza mediante resolución judicial o administrativa. En cualquier caso, la revocación efectiva del certificado se realiza en menos de 24 horas desde la recepción de la

solicitud de revocación en días hábiles administrativos y nunca superior a 72 horas en días inhábiles.

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

Como establezca la DPC de la PKI-SAR, en el numeral 4.9.6 Requisitos de verificación de las revocaciones por los terceros que confían.

4.9.7. FRECUENCIA DE EMISIÓN DE CRL

Como establezca la DPC de la PKI-SAR, en el numeral 4.9.7 Frecuencia de emisión de CRL.

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

Como establezca la DPC de la PKI-SAR, en el numeral 4.9.8 Tiempo máximo entre la generación y la publicación de las CRL.

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

Como establezca la DPC de la PKI-SAR, en el numeral 4.9.9 Disponibilidad de un sistema en línea de verificación del estado de los certificados.

4.9.10 REQUISITOS DE COMPROBACIÓN EN LÍNEA DE REVOCACIÓN

Como establece la DPC de la PKI-SAR, en el numeral 4.9.10 Requisitos de comprobación en línea de revocación.

4.9.11 OTRAS FORMAS DE DIVULGACIÓN DE INFORMACIÓN DE REVOCACIÓN DISPONIBLES

No estipulado.

4.9.12 CAUSAS PARA LA SUSPENSIÓN

Como establece la DPC de la PKI-SAR, en el numeral 4.9.12 Causas para la suspensión.

4.9.13 QUIÉN PUEDE SOLICITAR LA SUSPENSIÓN

La solicitud puede presentarla el titular del certificado o la institución a la cual pertenece mediante resolución administrativa, por medio de la Oficina de Talento Humano o la oficina que se haya designado como enlace en el convenio establecido con el SAR.

4.9.14 PROCEDIMIENTO PARA LA SOLICITUD DE SUSPENSIÓN

Se realiza el mismo proceso de revocación establecido en la presente PC, en el numeral 4.9.3. Procedimiento de solicitud de revocación.

4.9.15 LÍMITES DEL PERÏODO DE SUSPENSIÓN

Como establece la DPC de la PKI-SAR, en el numeral 4.9.15 Limites del periodo de suspensión.

4.10. SERVICIOS DE INFORMACIÓN DEL ESTADO DE CERTIFICADOS

4.10.1. CARACTERÍSTICAS OPERATIVAS

Como establece la DPC de la PKI-SAR, en el numeral 4.10.1 características operativas

4.10.2. DISPONIBILIDAD DEL SERVICIO

Como establece la DPC de la PKI-SAR, en el numeral 4.10.2 disponibilidad del servicio.

4.10.3. CARACTERÍSTICAS ADICIONALES

Como establece la DPC de la PKI-SAR, en el numeral 4.10.3. características adicionales.

4.11. FINALIZACIÓN DE LA VALIDEZ DE UN CERTIFICADO

Como establece la DPC de la PKI-SAR, en el numeral 4.11. finalización de la validez de un certificado.

4.12. CUSTODIA Y RECUPERACIÓN DE CLAVES

4.12.1. PRÁCTICAS Y POLÍTICAS DE RECUPERACIÓN DE CLAVES

La PKI-SAR no recupera la clave privada asociada al Certificado de Empleado(a) Público(a).

4.12.2. PRÁCTICAS Y POLÍTICAS DE RECUPERACIÓN DE CLAVES DE SESIÓN

No estipulado.

5. CONTROLES DE INSTALACIONES, GESTIÓN Y OPERACIONALES

5.1. CONTROLES FÍSICOS

5.1.1. UBICACIÓN FÍSICA Y CONSTRUCCIÓN

Como establece la DPC de la PKI-SAR, en el numeral 5.1.1 Ubicación física y construcción.

5.1.2. ACCESO FÍSICO

Como establece la DPC de la PKI-SAR, en el numeral 5.1.2 Acceso físico.

5.1.3. ELECTRICIDAD Y ACONDICIONADOR DE AIRES

Como establece la DPC de la PKI-SAR, en el numeral 5.1.3 Electricidad y Acondicionador de Aires.

5.1.4. EXPOSICIÓN AL AGUA

Como establece la DPC de la PKI-SAR, en el numeral 5.1.4 Exposición al agua.

5.1.5. PREVENCIÓN Y PROTECCIÓN DE INCENDIOS

Como establece la DPC de la PKI-SAR, en el numeral 5.1.5 Prevención y protección de incendios.

5.1.6. EQUIPOS DE ALMACENAMIENTO

Como establece la DPC de la PKI-SAR, en el numeral 5.1.6 Equipos de almacenamiento.

5.1.7. MANEJO DE RESIDUOS

Como establece la DPC de la PKI-SAR, en el numeral 5.1.7 Manejo de residuos.

5.1.8. COPIAS DE SEGURIDAD FUERA DE LAS INSTALACIONES

Como establece la DPC de la PKI-SAR, en el numeral 5.1.8 Copia de seguridad fuera de las instalaciones.

5.2. CONTROLES DE PROCEDIMIENTO

5.2.1. ROLES DE PKI-SAR

Como establece la DPC de la PKI-SAR, en el numeral 5.2.1 Roles de PKI-SAR.

5.2.2. NÚMERO DE PERSONAS REQUERIDAS POR TAREA

Como establece la DPC de la PKI-SAR, En el numeral 5.2.2 Número de personas requeridas por tarea.

5.2.3. ROLES QUE REQUIEREN SEGREGACIÓN DE FUNCIONES

Como establece la DPC de la PKI-SAR, en el numeral 5.2.3 Roles que requieren segregación de funciones.

5.3. CONTROLES DE PERSONAL

5.3.1. APTITUD, CONOCIMIENTO Y ACREDITACIÓN DE PROFESIONALES

Como establece la DPC de la PKI-SAR, en el numeral 5.3.1 Aptitud, conocimiento y acreditación de profesionales.

5.3.2. PROCESO PARA COMPROBACIÓN DE ANTECEDENTES

Como establece la DPC de la PKI-SAR, en el numeral 5.3.2 Proceso para comprobación de antecedentes.

5.3.3. REQUERIMIENTOS DE ENTRENAMIENTO

Como establece la DPC de la PKI-SAR, en el numeral 5.3.3 Requerimientos de formación.

5.3.4. REQUERIMIENTOS Y FRECUENCIA DE REENTRENAMIENTO

Como establece la DPC de la PKI-SAR, en el numeral 5.3.4 Requerimientos y frecuencia de reentrenamiento.

5.3.5. FRECUENCIA Y SECUENCIA DE ROTACIÓN DE OBLIGACIONES

Como establece la DPC de la PKI-SAR, en el numeral 5.3.5 Frecuencia y secuencia de rotación de obligaciones.

5.3.6. SANCIONES POR ACCIONES NO AUTORIZADAS

Como establece la DPC de la PKI-SAR, en el numeral 5.3.6 Sanciones por acciones no autorizadas.

5.3.7. REQUISITOS DE CONTRATACIÓN DE TERCEROS

Como establece la DPC de la PKI-SAR, en el numeral 5.3.7 Requisitos de contratación de terceros.

5.3.8. DOCUMENTACIÓN PROVISTA AL PERSONAL

Como establece la DPC de la PKI-SAR, en el numeral 5.3.8 Documentación provista al personal.

5.4. PROCEDIMIENTOS DE AUDITORÍA DE REGISTROS

5.4.1. TIPOS DE EVENTOS REGISTRADOS

Como establece la DPC de la PKI-SAR, en el numeral 5.4.1 Tipos de eventos registrados.

5.4.2. FRECUENCIA DE PROCESADO DE REGISTROS

Como establece la DPC de la PKI-SAR, en el numeral 5.4.2 Frecuencia de procesado de registros.

5.4.3. PERÍODO DE RETENCIÓN DE LOS REGISTROS DE AUDITORÍA

Como establece la DPC de la PKI-SAR, en el numeral 5.4.3 Período de Retención de los registros de Auditoría.

5.4.4. PROTECCIÓN DE LOS REGISTROS DE AUDITORÍA

Como establece la DPC de la PKI-SAR, en el numeral 5.4.4 Protección de los registros de auditoría.

5.4.5. PROCEDIMIENTOS DE RESPALDO DE LOS REGISTROS DE AUDITORIA

Como establece la DPC de la PKI-SAR, en el numeral 5.4.5 Procedimientos de respaldo de los registros de auditoría.

5.4.6. SISTEMA DE RECOLECCIÓN DE REGISTROS

Como establece la DPC de la PKI-SAR, en el numeral 5.4.6 Sistema de recolección de registros.

5.4.7. NOTIFICACIÓN AL SUJETO CAUSANTE DEL EVENTO

No estipulado.

5.4.8. ANÁLISIS DE VULNERABILIDADES

Como establece la DPC de la PKI-SAR, en el numeral 5.4.8 Análisis de Vulnerabilidades.

5.5. ARCHIVADO DE REGISTROS

5.5.1. TIPO DE EVENTOS ARCHIVADOS

Como establece la DPC de la PKI-SAR, en el numeral 5.5.1 Tipo de eventos archivados.

5.5.2. PERÍODO DE CONSERVACIÓN DE REGISTROS

Como establece la DPC de la PKI-SAR, en el numeral 5.5.2 Período de conservación de registros.

5.5.3. PROTECCIÓN DEL ARCHIVO

Como establece la DPC de la PKI-SAR, en el numeral 5.5.3 Protección del archivo.

5.5.4. PROCEDIMIENTOS DE COPIA DE RESPALDO DEL ARCHIVO

Como establece la DPC de la PKI-SAR, en el numeral 5.5.4 Procedimientos de copia de respaldo del archivo.

5.5.5. REQUISITO PARA EL SELLADO DE TIEMPO DE LOS REGISTROS

Como establece la DPC de la PKI-SAR, en el numeral 5.5.5 Requisito para el sellado de tiempo de los registros.

5.5.6. PROCEDIMIENTOS PARA OBTENER Y VERIFICAR INFORMACIÓN ARCHIVADA

Como establece la DPC de la PKI-SAR, en el numeral 5.5.6 Procedimientos para obtener y verificar información archivada.

5.6. CAMBIO DE CLAVES

Como establece la DPC de la PKI-SAR, en el numeral 5.6 Cambio de claves.

5.7. RECUPERACIÓN POR COMPROMISO DE CLAVE O CATÁSTROFE

5.7.1. GESTIÓN DE INCIDENTES Y VULNERABILIDADES

Como establece la DPC de la PKI-SAR, en el numeral 5.7.1 Gestión de incidentes y vulnerabilidades.

5.7.2. ACTUACIÓN ANTE DATOS Y SOFTWARE CORRUPTOS

Como establece la DPC de la PKI-SAR, en el numeral 5.7.2 Actuación ante datos y software corruptos.

5.7.3. PROCEDIMIENTO ANTE COMPROMISO DE CLAVE

Como establece la DPC de la PKI-SAR, en el numeral 5.7.3 Procedimiento ante compromiso de clave.

5.7.4. CONTINUIDAD DEL NEGOCIO DESPUÉS DE UN DESASTRE

Como establece la DPC de la PKI-SAR, en el numeral 5.7.4 Continuidad del negocio después de un desastre.

5.8. CESE DE UNA AUTORIDAD CERTIFICADORA (AC)

5.8.1. AUTORIDAD DE CERTIFICACIÓN

Como establece la DPC de la PKI-SAR, en el numeral 5.8.1 Autoridad de Certificación.

5.8.2. AUTORIDAD DE REGISTRO

Como establece la DPC de la PKI-SAR, en el numeral 5.8.2 Autoridad de Registro.

6. CONTROLES DE SEGURIDAD TÉCNICA

6.1. GENERACIÓN E INSTALACIÓN DEL PAR DE CLAVES

6.1.1. GENERACIÓN DEL PAR DE CLAVES

En relación con la generación de la clave del Suscriptor, la PKI-SAR no genera ni almacena la clave privada asociada al certificado expedido bajo la presente PC, que es generada bajo el exclusivo control del Suscriptor.

6.1.2. ENTREGA DE LA LLAVE PRIVADA AL SUSCRIPTOR

No existe ninguna entrega de clave privada en la emisión del certificado expedido bajo la presente PC. La clave privada asociada al Certificado de Empleado(a) Público(a) se genera bajo el control exclusivo del Suscriptor y custodiada en un archivo criptográfico PKCS12 para su uso.

6.1.3. ENTREGA DE LA CLAVE PÚBLICA AL EMISOR DEL CERTIFICADO

La clave pública, generada junto a la clave privada en el archivo PKCS12, se entrega a la AC mediante el envío de una solicitud de certificación.

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

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

6.1.5. TAMAÑO DE LAS CLAVES

El tamaño de las claves de los Certificados de Empleados(as) Públicos(as) es de 2048 bits, el algoritmo utilizado es RSA con SHA256.

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

La clave pública de los Certificados de Empleados(as) Públicos(as) de la PKI-SAR es codificada de acuerdo con RFC 3280 y PKCS#1 siendo el algoritmo de generación de claves RSA.

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

El uso admitido de la clave para el Certificado de Empleado(a) Públicos(a) está dado por el valor de las extensiones Key Usage y Extended Key Usage de los mismos. El contenido de dichas extensiones para cada uno de los tipos de Certificados de Empleado(a) Público(a) se puede consultar en el apartado 7.1.2. Extensión del Certificado del presente documento.

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

6.2.1. ESTÁNDARES PARA LOS MÓDULOS CRIPTOGRÁFICOS

Como establece la DPC de la PKI-SAR, en el numeral 6.2.1 Estándares para los módulos criptográficos.

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

La clave privada del Certificado de Empleado(a) Público(a) no se encuentra bajo control multipersonal. En ese sentido, el control de dicha clave privada recae enteramente sobre el Suscriptor.

6.2.3. RESGUARDO DE LA CLAVE PRIVADA

La custodia de la clave privada del Certificado de Empleado(a) Público(a) la realiza el Suscriptor de esta.

6.2.4. RESPALDO DE LA CLAVE PRIVADA

En ningún caso se realiza una copia de seguridad de la clave privada de firma de empleado(a) público(a), con la finalidad de garantizar el no repudio.

6.2.5. ARCHIVO DE LA CLAVE PRIVADA

La clave privada de firma de empleado(a) público(a) nunca es archivada para garantizar el no repudio.

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

En ningún caso es posible transferir la clave privada de firma de empleado(a) público(a) para garantizar el no repudio.

6.2.7. ALMACENAMIENTO DE LA CLAVE PRIVADA EN UN MÓDULO CRIPTOGRÁFICO

Las claves privadas de firma de empleados(as) públicos(as) se generan en un archivo criptográfico PKCS12, en el momento de la generación de los certificados.

6.2.8. MÉTODO DE ACTIVACIÓN DE LA CLAVE PRIVADA

La activación de la clave privada la efectúa el titular de esta, mediante el uso de su contraseña de firma (únicamente conocido por él).

6.2.9. MÉTODO DE DESACTIVACIÓN DE LA CLAVE PRIVADA

La desactivación de la clave privada de empleado(a) público(a) se realiza mediante solicitud del titular del certificado electrónico, por medio de la Oficina de Talento Humano o la oficina que se haya designado como enlace en el convenio establecido con el SAR. Esta desactivación se trata como una revocación del certificado electrónico, por lo que se sigue el procedimiento establecido para tal fin.

6.2.10. MÉTODO DE DESTRUCCIÓN DE LA CLAVE PRIVADA

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

6.2.11. CLASIFICACIÓN DE LOS MÓDULOS CRIPTOGRÁFICOS

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

6.3. OTROS ASPECTOS DE LA ADMINISTRACIÓN DEL PAR DE CLAVES

6.3.1. ARCHIVO DE LA CLAVE PÚBLICA

Como establece la DPC de la PKI-SAR en el numeral 6.3.1 Archivo de la clave pública.

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

El periodo de validez del certificado de empleado(a) público(a) es no mayor a 3 años desde el momento de emisión de este.

6.4. DATOS DE ACTIVACIÓN

6.4.1. INSTALACIÓN Y GENERACIÓN DE LOS DATOS DE ACTIVACIÓN

Como establece la DPC de la PKI-SAR, en el numeral 6.4.1 Instalación y generación de los datos de activación.

6.4.2. PROTECCIÓN PARA DATOS DE ACTIVACIÓN

Como establece la DPC de la PKI-SAR, en el numeral 6.4.2 Protección para datos de activación.

6.4.3. OTROS ASPECTOS REFERENTES A LOS DATOS DE ACTIVACIÓN

No estipulado.

6.5. CONTROLES DE SEGURIDAD INFORMÁTICA

6.5.1. REQUERIMIENTOS TÉCNICOS ESPECÍFICOS DE SEGURIDAD INFORMÁTICA

Como establece la DPC de la PKI-SAR, en el numeral 6.5.1 Requerimientos técnicos específicos de seguridad informática.

6.5.2. EVALUACIÓN DEL NIVEL DE SEGURIDAD INFORMÁTICA

Como establece la DPC de la PKI-SAR, en el numeral 6.5.2 Evaluación del nivel de seguridad informática.

6.6. CONTROLES TÉCNICOS DE CICLO DE VIDA

6.6.1. CONTROLES DE DESARROLLO DE SISTEMA

Como establece la DPC de la PKI-SAR, en el numeral 6.6.1 Controles de desarrollo de sistema.

6.6.2. CONTROLES DE ADMINISTRACIÓN DE SEGURIDAD

Como establece la DPC de la PKI-SAR, en el numeral 6.6.2 Controles de administración de seguridad.

6.6.3. CONTROLES DE SEGURIDAD DEL CICLO DE VIDA

Como establece la DPC de la PKI-SAR, en el numeral 6.6.3 Controles de seguridad del ciclo de vida.

6.7. CONTROLES DE SEGURIDAD DE REDES

Como establece la DPC de la PKI-SAR, en el numeral 6.7 Controles de seguridad de redes.

6.8. SELLADO DE TIEMPO

Como establece la DPC de la PKI-SAR, en el numeral 6.8 Sellado de tiempo.

6.9. OTROS CONTROLES ADICIONALES

6.9.1. CONTROL DE LA CAPACIDAD DE PRESTACIÓN DE LOS SERVICIOS

Como establece la DPC de la PKI-SAR, en el numeral 6.9.1 Control de la capacidad de prestación de los servicios.

6.9.2. CONTROL DE DESARROLLO DE SISTEMAS Y APLICACIONES INFORMÁTICAS

Como establece la DPC de la PKI-SAR, en el numeral 6.9.2 Control de desarrollo de sistemas y aplicaciones informáticas.

7. PERFILES DE CERTIFICADOS OCSP Y CRLS

7.1. PERFIL DE CERTIFICADO

7.1.1. NÚMERO DE VERSIÓN

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

7.1.2. EXTENSIONES DEL CERTIFICADO

A continuación, se detalla el contenido del Certificado de Firma Electrónica Avanzada de Empleado(a) Público(a):

Contenido del Certificado de Firma Electrónica Avanzada de Empleado(a) Público(a)				
Nombre	**Atributo**	**Valor**	**Obligatorio**	**Crítica**
Version	-	3	Si	-
Serial Number	-	25 BB 62 C0 77 28 C6 BE DA E0 8F 67 DC AB 4B 84 4C B4 02 DB	Si	-
Signature	Algorithm	Sha384WithRSAEncryption	Si	-
Issuer	CN	AUTORIDAD SUBORDINADA DEL SAR	Si	-
	O	SERVICIO DE ADMINISTRACION DE RENTAS	Si	-
	C	HN	Si	-

Contenido del Certificado de Firma Electrónica Avanzada de Empleado(a) Público(a)				
Nombre	**Atributo**	**Valor**	**Obligatorio**	**Crítica**
Validity	Not After	2023-02-28 12:42:52	Si	-
	Not Before	2033-02-28 12:42:52	Si	-
Subject	CN	CN=[F] NOMBRE <apellidos nombre> – ID <documento nacional de identidad/pasaporte>	Si	-
	O	EMPLEADO(A) PUBLICO(A)	Si	-
	C	HN	Si	-
	OU	FIRMA ELECTRONICA	Si	-
Subject Public Key Info	Algorithm	RSA	Si	-

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

Extensión del Certificado de Firma Electrónica Avanzada de Empleado(a) Público(a)				
Nombre	**Atributo**	**Valor**	**Obligatorio**	**Crítica**
Authority Key Identifier	-	<Resumen SHA-1 (160 bits) de la llave pública del campo Subject Public Key Info del emisor>	Si	No
Authority Key Identifier	-	<Resumen SHA-1 (160 bits) de la llave pública del campo Subject Public Key Info del emisor>	Si	No
Subject Key Identifier	-	<Resumen SHA-1 (160 bits) de la llave pública del campo Subject Public Key Info del emisor>	Si	No
Key Usage	-	digitalSignature, nonRepudiation	Si	Si
Extended Key Usage	-	-	Si	No

Extensión del Certificado de Firma Electrónica Avanzada de Empleado(a) Público(a)				
Nombre	**Atributo**	**Valor**	**Obligatorio**	**Crítica**
Certificate Policies	policyIdentifier (OID)	1.3.6.1.4.1.52089.2.4	Si	No
	cPSuri	URL: https://www.sar.gob.hn/firmaelectronica/		
Basic Constraints	Subject Type	End Entity	Si	Si
	Path Length Constraint	None	-	-
CRL Distribution Points	Distribution Point Name (URI)	<http://pki.sar.gob.hn/crlsar/crl.crl>	Si	
Authority Informatio n Access	cAIssuers (URI)	http://pki.sar.gob.hn/crlsar/casub.crt	Si	
	OCSP (URI)	http://ocsp2.sar.gob.hn/CryptosecOpenKey/va_service		

7.1.3. IDENTIFICADOR DE OBJETO (OID) DE LOS ALGORITMOS

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

7.1.4. FORMATO DE NOMBRES

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

7.1.5. RESTRICCIÓN DE LOS NOMBRES

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

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

El identificador de objeto de la Política de Certificado de Firma Electrónica Avanzada de Empleado(a) Público(a) es la definida en el apartado 1.2 Nombre del documento e identificación de la PC.

7.1.7. USO DE LA EXTENSIÓN "POLICY CONSTRAINTS"

La extensión Policy Constrains del Certificado Raíz de la AC no es utilizado.

7.1.8. SINTAXIS Y SEMÁNTICA DE LOS "POLICY QUALIFIER"

La extensión Certificate Policies contiene los siguientes Policy Qualifiers:

- URL CPS: contiene la URL, la DPC y la PC que rigen el certificado.
- Notice Reference: Nota de texto que se despliega en la pantalla, a instancia de una aplicación o persona, cuando un tercero verifica el certificado.

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

7.1.9. TRATAMIENTO SEMÁNTICO PARA LA EXTENSIÓN CRÍTICA "CERTIFICATE POLICIES"

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

7.2. PERFIL CRL

7.2.1. NÚMERO DE VERSIÓN

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

7.2.2. CRL Y EXTENSIONES

El perfil de la CRL sigue la siguiente estructura:

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

7.3. PERFIL DE OCSP

7.3.1. EXTENSIONES OCSP

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

7.3.2. EXTENSIONES OCSP

Como establece la DPC de la PKI-SAR, en el numeral 7.3.2 Extensiones OCSP.

8. AUDITORÍAS DE CUMPLIMIENTO Y OTROS CONTROLES

8.1. FRECUENCIA O CIRCUNSTANCIAS DE LOS CONTROLES PARA CADA AUTORIDAD

Como establece la DPC de la PKI-SAR, en el numeral 8.1 Frecuencia o circunstancias de los controles para cada Autoridad.

8.2. IDENTIFICACIÓN/CUALIFICACIÓN DEL AUDITOR

Como establece la DPC de la PKI-SAR, en el numeral 8.2 Identificación/cualificación del auditor.

8.3. RELACIÓN ENTRE EL AUDITOR Y LA AUTORIDAD AUDITADA

Como establece la DPC de la PKI-SAR, en el numeral 8.3 Relación entre el auditor y la autoridad auditada.

8.4. ASPECTOS CUBIERTOS POR LOS CONTROLES

Como establece la DPC de la PKI-SAR, en el numeral 8.4 Aspectos cubiertos por los controles.

8.5. TOMA DE DECISIONES FRENTE A LA DETECCIÓN DE DEFICIENCIAS

Como establece la DPC de la PKI-SAR, en el numeral 8.5 Toma de decisiones frente a la detección de deficiencias.

8.6. COMUNICACIÓN DE RESULTADOS

Como establece la DPC de la PKI-SAR, en el numeral 8.6 Comunicación de resultados.

9. OTROS ASPECTOS LEGALES Y DE ACTIVIDAD

9.1. TARIFAS

9.1.1. TARIFAS PARA EMISIÓN O RENOVACIÓN DE CERTIFICADO

Las tarifas de emisión y renovación de cada Certificado de Firma Electrónica Avanzada de Empleado(a) Público(a) no tiene ningún costo.

9.1.2. TARIFAS PARA ACCESO A CERTIFICADOS

No estipulado.

9.1.3. TARIFAS PARA ACCESO A INFORMACIÓN DE ESTADO O REVOCACIÓN

La PKI-SAR ofrece el servicio de información del estado del certificado a través de CRL o del OCSP de forma gratuita.

9.1.4. TARIFAS PARA OTROS SERVICIOS

Como establece la DPC de la PKI-SAR, en el numeral 9.1.4. Tarifas para otros servicios.

9.1.5. POLÍTICA DE REEMBOLSO

Al no aplicar una tarifa del servicio del ciclo de vida de un Certificado de Firma Electrónica Avanzada de Empleado(a) Público(a), el PKI-SAR no realizara ningún reembolso.

9.2. RESPONSABILIDADES ECONÓMICAS

9.2.1. SEGURO DE RESPONSABILIDAD CIVIL

Como establece la DPC de la PKI-SAR, en el numeral 9.2.1 Seguro de responsabilidad civil.

9.2.2. OTROS ACTIVOS

No estipulado.

9.2.3. SEGUROS Y GARANTÍAS PARA ENTIDADES FINALES

No estipulado.

9.3. CONFIDENCIALIDAD DE LA INFORMACIÓN

Como establece la DPC de la PKI-SAR, en el numeral 9.3 Confidencialidad de la información.

9.3.1. ALCANCE DE LA INFORMACIÓN CONFIDENCIAL

Como establece la DPC de la PKI-SAR, en el numeral 9.3.1 Alcance de la información confidencial.

9.3.2. INFORMACIÓN NO CONFIDENCIAL

Como establece la DPC de la PKI-SAR, en el numeral 9.3.2 Información no confidencial.

9.3.3. RESPONSABILIDAD DE PROTEGER LA INFORMACIÓN CONFIDENCIAL

Como establece la DPC de la PKI-SAR, en el numeral 9.3.3 Responsabilidad de proteger la información confidencial.

9.4. PROTECCIÓN DE LA INFORMACIÓN PERSONAL

Como establezca la DPC de la PKI-SAR, en el numeral 9.4 Protección de la información personal.

9.5. DERECHOS DE PROPIEDAD INTELECTUAL

Como establece la DPC de la PKI-SAR, en el numeral 9.5 Derechos de propiedad intelectual.

9.6. OBLIGACIONES Y GARANTÍAS

9.6.1. OBLIGACIONES DE LA AC

Como establece la DPC de la PKI-SAR, en el numeral 9.6.1 Obligaciones de las AC.

9.6.2. OBLIGACIONES DE LA AR

Como establece la DPC de la PKI-SAR, en el numeral 9.6.2 Obligaciones de la AR.

9.6.3. OBLIGACIONES DE LOS SUSCRIPTORES DE LOS CERTIFICADOS

Como establece la DPC de la PKI-SAR, en el numeral 9.6.3 Obligaciones de los Suscriptores de los certificados.

9.6.4. OBLIGACIONES DE LOS TERCEROS QUE CONFÍAN O ACEPTEN LOS CERTIFICADOS

Como establece la DPC de la PKI-SAR, en el numeral 9.6.4 Obligaciones de los terceros que confían o acepten los certificados.

9.7. EXENCIÓN DE RESPONSABILIDADES

Como establece la DPC de la PKI-SAR, en el numeral 9.7 Exención de responsabilidades.

9.8. LIMITACIONES DE LAS RESPONSABILIDADES

Como establece la DPC de la PKI-SAR, en el numeral 9.8 Limitaciones de las responsabilidades.

9.9. INDEMNIZACIONES

Como establece la DPC de la PKI-SAR, en el numeral 9.9 Indemnizaciones.

9.9.1. INDEMNIZACIONES DE LA CA

No estipulado.

9.9.2. INDEMNIZACIONES DE LOS SUSCRIPTORES

No estipulado.

9.9.3. INDEMNIZACIONES DE LAS PARTES QUE CONFÍAN

No estipulado.

9.10. PERÍODO DE VALIDEZ DE ESTE DOCUMENTO

9.10.1. PERIODO

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

9.10.2. TERMINACIÓN DE LA DPC

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

Cuando la DPC quede derogada, la misma debe ser eliminada de los repositorios de PKI-SAR, conservando el archivo durante cinco (5) años.

9.10.3. EFECTOS DE LA TERMINACIÓN

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

9.11. NOTIFICACIONES INDIVIDUALES Y COMUNICACIONES CON LOS PARTICIPANTES

Como establece la DPC de la PKI-SAR, en el numeral 9.11 Notificaciones individuales y comunicaciones con los participantes.

9.12. MODIFICACIONES DE ESTE DOCUMENTO

9.12.1. PROCEDIMIENTO PARA LAS MODIFICACIONES

Como establece la DPC de la PKI-SAR, en el numeral 9.12.1 Procedimiento para las modificaciones.

9.12.2. PERIODO Y MECANISMO DE NOTIFICACIÓN

Como establece la DPC de la PKI-SAR, en el numeral 9.12.2 Periodo y mecanismo de notificación.

9.12.3. CIRCUNSTANCIAS EN EL QUE EL OID DEBE SER CAMBIADO

Como establece la DPC de la PKI-SAR, en el numeral 9.12.3 Circunstancias bajo las cuales debe cambiarse un OID.

9.13. RESOLUCIÓN DE CONFLICTOS

Como establece la DPC de la PKI-SAR, en el numeral 9.13 Resolución de Conflictos.

9.14. NORMATIVA APLICABLE

Como establece la DPC de la PKI-SAR, en el numeral 9.14 Normativa aplicable.

9.15. CUMPLIMIENTO DE LA LEGISLACIÓN APLICABLE

Como establece la DPC de la PKI-SAR, en el numeral 9.15 Cumplimiento de la legislación aplicable.

9.16. ESTIPULACIONES MISCELÁNEAS

9.16.1. ACEPTACIÓN DE LA DPC

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

9.16.2. RESOLUCIÓN DE CONFLICTOS EN LA VÍA JUDICIAL

Como establece la DPC de la PKI-SAR, en el numeral 19.16.2 Resolución de conflictos en la vía judicial

9.17. OTRAS ESTIPULACIONES

No se consideran otras estipulaciones.