



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

POL-GIF-GGI-NDP-019-V2

SAR
SERVICIO DE ADMINISTRACIÓN DE RENTAS

DIRECCIÓN EJECUTIVA
SECRETARIA GENERAL

Febrero 2023

	POLÍTICA DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN DE INFRAESTRUCTURA DE CLAVE PÚBLICA DEL SERVICIO DE ADMINISTRACIÓN DE RENTAS DE LA REPUBLICA DE HONDURAS SECRETARÍA GENERAL	Código: POL-GIF-GGI-NDP-019- V2 Fecha de vigencia: FEBRERO - 2023
---	---	---

FECHA VIGENCIA: ENERO 2023	CÓDIGO: POL-GIF-GGI-NDP-019-V2	VERSIÓN 2.0	N° PÁGINAS 4
--	--	-------------------------------	--------------------------------

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

RUBRO	CARGO	FIRMA
APROBADO POR:	Lic. Marlon David Ochoa Martínez Director Ejecutivo	
	Lic. Christian David Duarte Chávez Sub Director Ejecutivo	
	Abg. Nidia Saraí Berrios Martínez Secretaría General	
	Ing. Diana Orestila Cárcamo Rodríguez Directora Nacional de Tecnología	
	Lic. Alessandra Díaz Tovar Directora Nacional de Gestión Estratégica	
	Abg. Gersson Orlando Sierra Portillo Director Nacional Jurídica	

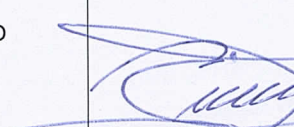
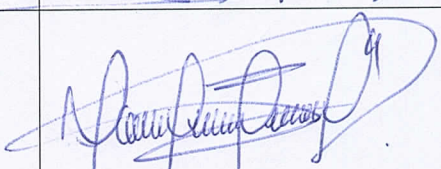
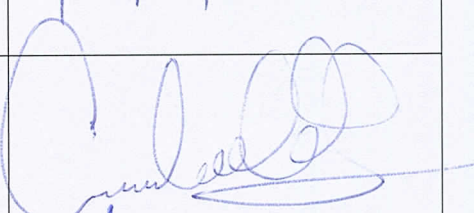
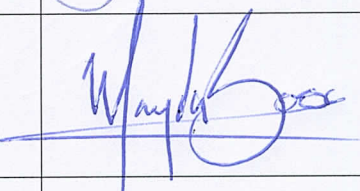
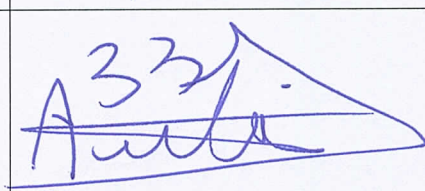


**POLÍTICA DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN
DE INFRAESTRUCTURA DE CLAVE PÚBLICA DEL SERVICIO DE
ADMINISTRACIÓN DE RENTAS DE LA REPUBLICA DE
HONDURAS**

SECRETARÍA GENERAL

Código:
POL-GIF-GGI-NDP-019-
V2

Fecha de vigencia:
FEBRERO - 2023

	Abg. Calvin Antonio Ruíz Lobo Inspector General	 
REVISIÓN:	Abg. Fátima Isabel Estrada Saravia Experta en el departamento de Asesoría Legal	
	Abg. Carlos Antonio García García Especialista de Secretaría General	
	Abg. Mayda Areli Sosa Alvarez Experta en el Departamento de Procuración Legal	
ELABORADO POR:	Ing. Osman René Moreno Ramos Experto de 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 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.

Se prohíbe cualquier reproducción, distribución o comunicado público que refiera a este documento institucional, sin autorización expresa del Servicio de Administración de Rentas.

	POLÍTICA DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN DE INFRAESTRUCTURA DE CLAVE PÚBLICA DEL SERVICIO DE ADMINISTRACIÓN DE RENTAS DE LA REPUBLICA DE HONDURAS SECRETARÍA GENERAL	Código: POL-GIF-GGI-NDP-019- V2 Fecha de vigencia: FEBRERO - 2023
---	---	---

Contenido

1.	INTRODUCCIÓN	15
1.1	VISIÓN GENERAL	15
1.1.1	CONTROL DEL DOCUMENTO	15
1.1.2	OBJETIVO VINCULADO AL DOCUMENTO.....	16
1.1.3	DOCUMENTO RELACIONADO	16
1.1.4	IDENTIFICACIÓN DEL PROCESO	16
1.1.5	OBJETIVO	16
1.1.6	ALCANCE	17
1.1.7	NORMAS Y DISPOSICIONES.....	17
1.1.8	EXCLUSIONES	17
1.1.9	MARCO NORMATIVO	18
1.1.10	REFERENCIA TÉCNICA	18
1.2	NOMBRE DEL DOCUMENTO E IDENTIFICACIÓN DE LA DPC	18
1.3	PARTICIPANTES DE LA PKI-SAR.....	19
1.3.1	AUTORIDAD DE CERTIFICACIÓN (AC).....	20
1.3.2	AUTORIDAD CERTIFICADORA RAÍZ DEL SAR	21
1.3.3	AUTORIDAD CERTIFICADORA SUBORDINADA DEL SAR	22
1.3.4	AUTORIDAD DE REGISTRO (AR)	23
1.3.5	AUTORIDAD DE VALIDACIÓN (AV)	23
1.3.6	AUTORIDAD DE SELLADO DE TIEMPO (AST)	24
1.3.7	SOLICITANTES Y SUSCRIPTORES DE CERTIFICADOS	24
1.3.8	TERCEROS QUE CONFÍAN EN LOS CERTIFICADOS EMITIDOS POR LA PKI-SAR	25
1.3.9	AUTORIDAD ADMINISTRATIVA COMPETENTE (AAC)	25
1.3.10	PRESTADOR DE SERVICIOS DE CERTIFICACIÓN (PSC).....	25
1.4	USO DE LOS CERTIFICADOS	27
1.4.1	USO ADECUADO DE LOS CERTIFICADOS	27
1.4.2	PROHIBICIONES DE USO DE LOS CERTIFICADOS.....	27
1.5	ADMINISTRACIÓN DE LAS POLÍTICAS	28
1.5.1	ORGANIZACIÓN RESPONSABLE DE LA DPC	28

	POLÍTICA DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN DE INFRAESTRUCTURA DE CLAVE PÚBLICA DEL SERVICIO DE ADMINISTRACIÓN DE RENTAS DE LA REPUBLICA DE HONDURAS SECRETARÍA GENERAL	Código: POL-GIF-GGI-NDP-019- V2 Fecha de vigencia: FEBRERO - 2023
---	---	---

1.5.2	PROCEDIMIENTO DE APROBACIÓN Y MODIFICACIÓN DE LA DPC	28
1.5.3	RESPONSABLE POR MODIFICACIONES A LA DPC	28
1.5.4	DATOS DE CONTACTO.....	29
1.6	GLOSARIO Y SIGLAS.....	30
1.6.1	GLOSARIO	30
1.6.2	SIGLAS	34
2.	REPOSITORIOS Y PUBLICACIÓN DE INFORMACIÓN	36
2.1	REPOSITORIOS	36
2.2	PUBLICACIÓN DE INFORMACIÓN DE CERTIFICACIÓN.....	36
2.3	TIEMPOS Y FRECUENCIA DE PUBLICACIÓN	37
2.4	CONTROLES DE ACCESO A LOS REPOSITORIOS	37
3.	IDENTIFICACIÓN Y AUTENTICACIÓN.....	37
3.1	NOMBRES	37
3.1.1	TIPOS DE NOMBRES	37
3.1.2	NECESIDAD DE QUE LOS NOMBRES SEAN SIGNIFICATIVOS.	38
3.1.3	REGLA PARA INTERPRETAR VARIOS FORMATOS DE NOMBRES	38
3.1.4	UNICIDAD DE LOS NOMBRES	38
3.1.5	RECONOCIMIENTO, AUTENTICACIÓN Y PAPEL DE LAS MARCAS REGISTRADAS.....	38
3.2	VALIDACIÓN INICIAL DE IDENTIDAD	39
3.2.1	MÉTODOS PARA COMPROBAR LA CLAVE PRIVADA.....	39
3.2.2	AUTENTICACIÓN DE LA IDENTIDAD DE LA ORGANIZACIÓN ...	39
3.2.3	AUTENTICACIÓN DE LA IDENTIDAD DE LA PERSONA FÍSICA SOLICITANTE	39
3.2.4	INFORMACIÓN NO VERIFICADA SOBRE EL SOLICITANTE	39
3.2.5	COMPROBACIÓN DE LAS FACULTADES DE REPRESENTACIÓN	39
3.2.6	CRITERIOS PARA INTEROPERABILIDAD.....	39
3.3	IDENTIFICACIÓN Y AUTENTICACIÓN PARA SOLICITUDES DE RENOVACIÓN	40

	POLÍTICA DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN DE INFRAESTRUCTURA DE CLAVE PÚBLICA DEL SERVICIO DE ADMINISTRACIÓN DE RENTAS DE LA REPUBLICA DE HONDURAS SECRETARÍA GENERAL	Código: POL-GIF-GGI-NDP-019- V2 Fecha de vigencia: FEBRERO - 2023
---	---	---

4.	REQUISITOS OPERACIONALES PARA EL CICLO DE VIDA DE LOS CERTIFICADOS	40
4.1	SOLICITUD DE CERTIFICADOS	40
4.1.1	¿QUIEN PUEDE REALIZAR UNA SOLICITUD?	40
4.1.2	PROCESO DE ENROLAMIENTO Y RESPONSABILIDADES DE LOS SOLICITANTES.....	41
4.2	GESTIÓN DE LAS SOLICITUDES DE CERTIFICADOS	41
4.2.1	FUNCIONES DE IDENTIFICACIÓN Y AUTENTICACIÓN.....	41
4.2.2	RECHAZO O ACEPTACIÓN DE SOLICITUDES DE CERTIFICADO 41	
4.2.3	PLAZO PARA LA GESTIÓN DE LAS SOLICITUDES	42
4.3	EMISIÓN DE CERTIFICADOS	42
4.3.1	ACCIONES DE LA AC DURANTE LA EMISIÓN DE CERTIFICADO. 42	
4.3.2	NOTIFICACIÓN AL SOLICITANTE DE LA EMISIÓN POR LA AC DEL CERTIFICADO	42
4.4	ACEPTACIÓN DEL CERTIFICADO	43
4.4.1	ACCIÓN QUE AFIRMA LA ACEPTACIÓN DEL CERTIFICADO	43
4.4.2	PUBLICACIÓN DEL CERTIFICADO POR PARTE DE LA AC.....	43
4.4.3	NOTIFICACIÓN DE LA EMISIÓN DEL CERTIFICADO POR LA AC A OTRAS ENTIDADES.....	43
4.5	USO DEL PAR DE CLAVES Y CERTIFICADO	43
4.5.1	USO DE LA CLAVE PRIVADA Y DEL CERTIFICADO POR EL SUSCRIPTOR	43
4.5.2	USO DE LA CLAVE PÚBLICA Y DEL CERTIFICADO POR LO TERCEROS QUE CONFÍAN.....	44
4.6	RENOVACIÓN DE CERTIFICADOS SIN CAMBIO DE CLAVE.....	44
4.6.1	CIRCUNSTANCIAS PARA LA RENOVACIÓN DE CERTIFICADOS SIN CAMBIO DE CLAVE AUSENTE	44
4.6.2	GESTIÓN DE LAS PETICIONES DE RENOVACIÓN DE CERTIFICADOS SIN CAMBIO DE CLAVES.....	44
4.6.3	QUIÉN PUEDE SOLICITAR LA RENOVACIÓN DE LOS CERTIFICADOS SIN CAMBIO DE CLAVE	45



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

SECRETARÍA GENERAL

Código:
POL-GIF-GGI-NDP-019-
V2

Fecha de vigencia:
FEBRERO - 2023

4.6.4	NOTIFICACIÓN DE LA EMISIÓN DE UN NUEVO CERTIFICADO AL SUScriptor	45
4.6.5	FORMA DE ACEPTACIÓN DEL CERTIFICADO SIN CAMBIO DE CLAVE AUSENTE	45
4.6.6	PUBLICACIÓN DEL CERTIFICADO SIN CAMBIO DE CLAVE AUSENTE	45
4.6.7	NOTIFICACIÓN DE LA EMISIÓN DEL CERTIFICADO POR LA AC A OTRAS AUTORIDADES	45
4.7	RENOVACIÓN DE CERTIFICADOS CON CAMBIO DE CLAVES	45
4.7.1	CIRCUNSTANCIAS PARA LA RENOVACIÓN CON CAMBIO DE CLAVES DE UN CERTIFICADO	45
4.7.2	QUIÉN PUEDE PEDIR LA RENOVACIÓN DE LOS CERTIFICADOS	46
4.7.3	GESTIÓN DE LAS PETICIONES DE RENOVACIÓN DE CERTIFICADOS CON CAMBIO DE CLAVES	46
4.7.4	NOTIFICACIÓN DE LA EMISIÓN DE UN NUEVO CERTIFICADO AL SUScriptor	46
4.7.5	MÉTODO DE ACEPTACIÓN DEL CERTIFICADO CON CAMBIO DE CLAVES	46
4.7.6	PUBLICACIÓN DEL CERTIFICADO CON LAS NUEVAS CLAVES POR PARTE DE LA AC	47
4.7.7	NOTIFICACIÓN DE LA EMISIÓN DEL CERTIFICADO POR LA AC A OTRAS AUTORIDADES	47
4.8	MODIFICACIÓN DE CERTIFICADOS	47
4.8.1	CIRCUNSTANCIAS PARA LA MODIFICACIÓN DEL CERTIFICADO	47
4.8.2	QUIÉN PUEDE SOLICITAR LA MODIFICACIÓN DE LOS CERTIFICADOS	47
4.8.3	GESTIÓN DE LAS PETICIONES DE MODIFICACIÓN DE CERTIFICADOS	47
4.8.4	NOTIFICACIÓN POR LA EMISIÓN DE UN CERTIFICADO MODIFICADO AL SUScriptor	47
4.8.5	MÉTODO DE ACEPTACIÓN DEL CERTIFICADO MODIFICADO	48
4.8.6	PUBLICACIÓN DEL CERTIFICADO MODIFICADO POR LA CA...	48

	POLÍTICA DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN DE INFRAESTRUCTURA DE CLAVE PÚBLICA DEL SERVICIO DE ADMINISTRACIÓN DE RENTAS DE LA REPUBLICA DE HONDURAS SECRETARÍA GENERAL	Código: POL-GIF-GGI-NDP-019- V2 Fecha de vigencia: FEBRERO - 2023
---	---	---

4.8.7	NOTIFICACIÓN DE LA MODIFICACIÓN DEL CERTIFICADO POR LA CA A OTRAS ENTIDADES	48
4.9	REVOCACIÓN Y SUSPENSIÓN DE CERTIFICADOS	48
4.9.1	CIRCUNSTANCIAS PARA LA REVOCACIÓN	48
4.9.2	¿QUIÉN PUEDE SOLICITAR LA REVOCACIÓN?	49
4.9.3	PROCEDIMIENTO DE SOLICITUD DE REVOCACIÓN	50
4.9.4	PERIODO EN QUE SE DEBE PROCESAR LAS SOLICITUDES DE REVOCACIÓN	50
4.9.5	PLAZO EN EL QUE SE DEBE RESOLVER LA SOLICITUD DE REVOCACIÓN	50
4.9.6	REQUISITOS DE VERIFICACIÓN DE LAS REVOCAIONES POR LOS TERCEROS QUE CONFÍAN	51
4.9.7	FRECUENCIA DE EMISIÓN DE CRL	51
4.9.8	TIEMPO MÁXIMO ENTRE LA GENERACIÓN Y LA PUBLICACIÓN DE LAS CRL	51
4.9.9	DISPONIBILIDAD DE UN SISTEMA EN LÍNEA DE VERIFICACIÓN DEL ESTADO DE LOS CERTIFICADOS	52
4.9.10	REQUISITOS DE COMPROBACIÓN EN LÍNEA DE REVOCACIÓN	52
4.9.11	OTRAS FORMAS DE DIVULGACIÓN DE INFORMACIÓN DE REVOCACIÓN DISPONIBLES	52
4.9.12	CAUSAS PARA LA SUSPENSIÓN	52
4.9.13	QUIÉN PUEDE SOLICITAR LA SUSPENSIÓN	53
4.9.14	PROCEDIMIENTO PARA LA SOLICITUD DE SUSPENSIÓN	53
4.9.15	LÍMITES DEL PERIODO DE SUSPENSIÓN	53
4.10	SERVICIOS DE INFORMACIÓN DEL ESTADO DE CERTIFICADOS	53
4.10.1	CARACTERÍSTICAS OPERATIVAS	53
4.10.2	DISPONIBILIDAD DEL SERVICIO	54
4.10.3	CARACTERÍSTICAS ADICIONALES	54
4.11	FINALIZACIÓN DE LA VALIDEZ DE UN CERTIFICADO	54
4.12	CUSTODIA Y RECUPERACIÓN DE CLAVES	55
4.12.1	PRÁCTICAS Y POLÍTICAS DE RECUPERACIÓN DE CLAVES	55



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

SECRETARÍA GENERAL

Código:
POL-GIF-GGI-NDP-019-
V2

Fecha de vigencia:
FEBRERO - 2023

4.12.2	PRÁCTICAS Y POLÍTICAS DE RECUPERACIÓN DE CLAVES DE SESIÓN	55
5.	CONTROLES DE INSTALACIONES, GESTIÓN Y OPERACIONALES	55
5.1	CONTROLES FÍSICOS	55
5.1.1	UBICACIÓN FÍSICA Y CONSTRUCCIÓN	55
5.1.2	ACCESO FÍSICO	56
5.1.3	ELECTRICIDAD Y ACONDICIONADOR DE AIRES	56
5.1.4	EXPOSICIÓN AL AGUA	56
5.1.5	PREVENCIÓN Y PROTECCIÓN DE INCENDIOS	57
5.1.6	EQUIPOS DE ALMACENAMIENTO	57
5.1.7	MANEJO DE RESIDUOS	57
5.1.8	COPIA DE SEGURIDAD FUERA DE LAS INSTALACIONES	57
5.2	CONTROLES DE PROCEDIMIENTO	57
5.2.1	ROLES DE PKI-SAR	58
5.2.2	NÚMERO DE PERSONAS REQUERIDAS POR TAREA	59
5.2.3	ROLES QUE REQUIEREN SEGREGACIÓN DE FUNCIONES	59
5.3	CONTROLES DE PERSONAL	59
5.3.1	APTITUD, CONOCIMIENTO Y ACREDITACIÓN DE PROFESIONALES	59
5.3.2	PROCESO PARA COMPROBACIÓN DE ANTECEDENTES	59
5.3.3	REQUERIMIENTOS DE FORMACIÓN	60
5.3.4	REQUERIMIENTOS Y FRECUENCIA DE REENTRENAMIENTO	60
5.3.5	FRECUENCIA Y SECUENCIA DE ROTACIÓN DE OBLIGACIONES	60
5.3.6	SANCIONES POR ACCIONES NO AUTORIZADAS	61
5.3.7	REQUISITOS DE CONTRATACIÓN DE TERCEROS	61
5.3.8	DOCUMENTACIÓN PROVISTA AL PERSONAL	61
5.4	PROCEDIMIENTOS DE AUDITORÍA DE REGISTROS	62
5.4.1	TIPOS DE EVENTOS REGISTRADOS	62
5.4.2	FRECUENCIA DE PROCESADO DE REGISTROS	62
5.4.3	PERÍODO DE RETENCIÓN DE LOS REGISTROS DE AUDITORÍA	63

	POLÍTICA DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN DE INFRAESTRUCTURA DE CLAVE PÚBLICA DEL SERVICIO DE ADMINISTRACIÓN DE RENTAS DE LA REPUBLICA DE HONDURAS SECRETARÍA GENERAL	Código: POL-GIF-GGI-NDP-019- V2 Fecha de vigencia: FEBRERO - 2023
---	---	---

5.4.4	PROTECCIÓN DE LOS REGISTROS DE AUDITORÍA	63
5.4.5	PROCEDIMIENTOS DE RESPALDO DE LOS REGISTROS DE AUDITORÍA	63
5.4.6	SISTEMA DE RECOLECCIÓN DE REGISTROS	63
5.4.7	NOTIFICACIÓN AL SUJETO CAUSANTE DEL EVENTO	63
5.4.8	ANÁLISIS DE VULNERABILIDADES	63
5.5	ARCHIVADO DE REGISTROS	64
5.5.1	TIPO DE EVENTOS ARCHIVADOS	64
5.5.2	PERÍODO DE CONSERVACIÓN DE REGISTROS	64
5.5.3	PROTECCIÓN DEL ARCHIVO	64
5.5.4	PROCEDIMIENTOS DE COPIA DE RESPALDO DEL ARCHIVO	65
5.5.5	REQUISITO PARA EL SELLADO DE TIEMPO DE LOS REGISTROS 65	
5.5.6	PROCEDIMIENTOS PARA OBTENER Y VERIFICAR INFORMACIÓN ARCHIVADA	65
5.6	CAMBIO DE CLAVES	65
5.7	RECUPERACIÓN POR COMPROMISO DE CLAVE O CATÁSTROFE	66
5.7.1	GESTIÓN DE INCIDENTES Y VULNERABILIDADES	66
5.7.2	ACTUACIÓN ANTE DATOS Y SOFTWARE CORRUPTOS	66
5.7.3	PROCEDIMIENTO ANTE COMPROMISO DE CLAVE	66
5.7.4	CONTINUIDAD DEL NEGOCIO DESPUÉS DE UN DESASTRE	67
5.8	CESE DE UNA AUTORIDAD CERTIFICADORA (AC)	67
5.8.1	AUTORIDAD DE CERTIFICACIÓN	67
5.8.2	AUTORIDAD DE REGISTRO	68
6.	CONTROLES DE SEGURIDAD TÉCNICA	68
6.1	GENERACIÓN E INSTALACIÓN DEL PAR DE CLAVES	68
6.1.1	GENERACIÓN DEL PAR DE CLAVES	68
6.1.2	ENTREGA DE LA LLAVE PRIVADA AL SUScriptor	68
6.1.3	ENTREGA DE LA CLAVE PÚBLICA AL EMISOR DEL CERTIFICADO	69
6.1.4	ENTREGA DE LA CLAVE PÚBLICA DE LA AC A LOS TERCEROS QUE CONFÍAN	69



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

SECRETARÍA GENERAL

Código:
POL-GIF-GGI-NDP-019-
V2

Fecha de vigencia:
FEBRERO - 2023

6.1.5	TAMAÑO DE LAS CLAVES.....	69
6.1.6	PARÁMETROS DE GENERACIÓN DE LA CLAVE PÚBLICA Y ASEGURAMIENTO DE LA CALIDAD	69
6.1.7	USOS ADMITIDOS DE LA CLAVE (CAMPO KEYUSAGE DE X.509 V3) 70	
6.2	PROTECCIÓN DE LA CLAVE PRIVADA Y CONTROLES DE INGENIERÍA DE LOS MÓDULOS	70
6.2.1	ESTÁNDARES PARA LOS MÓDULOS CRIPTOGRÁFICOS.....	70
6.2.2	CONTROL MULTIPERSONA (K DE N) DE LA CLAVE PRIVADA .	71
6.2.3	RESGUARDO DE LA CLAVE PRIVADA	71
6.2.4	RESPALDO DE LA CLAVE PRIVADA.....	71
6.2.5	ARCHIVO DE LA CLAVE PRIVADA.....	71
6.2.6	TRANSFERENCIA DE LA CLAVE PRIVADA HACIA O DESDE UN MÓDULO CRIPTOGRÁFICO	71
6.2.7	ALMACENAMIENTO DE LA CLAVE PRIVADA EN UN MÓDULO CRYPTOGRÁFICO	71
6.2.8	MÉTODO DE ACTIVACIÓN DE LA CLAVE PRIVADA.....	72
6.2.9	MÉTODO DE DESACTIVACIÓN DE LA CLAVE PRIVADA	72
6.2.10	MÉTODO DE DESTRUCCIÓN DE LA CLAVE PRIVADA	72
6.2.11	CLASIFICACIÓN DE LOS MÓDULOS CRIPTOGRÁFICOS	72
6.3	OTROS ASPECTOS DE LA ADMINISTRACIÓN DEL PAR DE CLAVES.....	72
6.3.1	ARCHIVO DE LA CLAVE PÚBLICA	72
6.3.2	PERÍODOS OPERATIVOS DE LOS CERTIFICADOS Y PERÍODO PARA USO DEL PAR DE CLAVES.....	73
6.4	DATOS DE ACTIVACIÓN	73
6.4.1	INSTALACIÓN Y GENERACIÓN DE LOS DATOS DE ACTIVACIÓN 73	
6.4.2	PROTECCIÓN PARA DATOS DE ACTIVACIÓN	73
6.4.3	OTROS ASPECTOS REFERENTES A LOS DATOS DE ACTIVACIÓN.....	74
6.5	CONTROLES DE SEGURIDAD INFORMÁTICA.....	74
6.5.1	REQUERIMIENTOS TÉCNICOS ESPECÍFICOS DE SEGURIDAD INFORMÁTICA.....	74
6.5.2	EVALUACIÓN DEL NIVEL DE SEGURIDAD INFORMÁTICA.....	74

	POLÍTICA DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN DE INFRAESTRUCTURA DE CLAVE PÚBLICA DEL SERVICIO DE ADMINISTRACIÓN DE RENTAS DE LA REPUBLICA DE HONDURAS SECRETARÍA GENERAL	Código: POL-GIF-GGI-NDP-019- V2 Fecha de vigencia: FEBRERO - 2023
---	---	---

6.6	CONTROLES DE SEGURIDAD DEL CICLO DE VIDA.....	74
6.6.1	CONTROLES DE DESARROLLO DE SISTEMA.....	74
6.6.2	CONTROLES DE ADMINISTRACIÓN DE SEGURIDAD.....	75
6.6.3	CONTROLES DE SEGURIDAD DEL CICLO DE VIDA	75
6.7	CONTROLES DE SEGURIDAD DE REDES	75
6.8	SELLADO DE TIEMPO	75
6.9	OTROS CONTROLES ADICIONALES.....	76
6.9.1	CONTROL DE LA CAPACIDAD DE PRESTACIÓN DE LOS SERVICIOS.....	76
6.9.2	CONTROL DE DESARROLLO DE SISTEMAS Y APLICACIONES INFORMÁTICAS.....	76
7.	PERFILES DE CERTIFICADOS OCSP Y CRLS	76
7.1	PERFIL DE CERTIFICADO.....	76
7.1.1	NÚMERO DE VERSIÓN	76
7.1.2	EXTENSIONES DEL CERTIFICADO	76
7.1.3	IDENTIFICADOR DE OBJETO (OID) DE LOS ALGORITMOS	78
7.1.4	FORMATO DE NOMBRES.....	79
7.1.5	RESTRICCIÓN DE LOS NOMBRES	79
7.1.6	IDENTIFICADOR DE OBJETO (OID) DE LAS POLÍTICAS DE CERTIFICACIÓN.....	79
7.1.7	USO DE LA EXTENSIÓN “POLICYCONSTRAINTS”	79
7.1.8	SINTAXIS Y SEMÁNTICA DE LOS “POLICYQUALIFIER”	79
7.1.9	TRATAMIENTO SEMÁNTICO PARA LA EXTENSIÓN CRÍTICA “CERTIFICATEPOLICIES”	80
7.2	PERFIL CRL.....	80
7.2.1	NÚMERO DE VERSIÓN	80
7.2.2	CRL Y EXTENSIONES	80
7.3	PERFIL DE OCSP	81
7.3.1	NÚMERO DE VERSIÓN	81
7.3.2	EXTENSIONES OCSP	81
8.	AUDITORÍAS DE CUMPLIMIENTO Y OTROS CONTROLES	81
8.1	FRECUENCIA O CIRCUNSTANCIAS DE LOS CONTROLES PARA CADA AUTORIDAD	81

	POLÍTICA DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN DE INFRAESTRUCTURA DE CLAVE PÚBLICA DEL SERVICIO DE ADMINISTRACIÓN DE RENTAS DE LA REPUBLICA DE HONDURAS SECRETARÍA GENERAL	Código: POL-GIF-GGI-NDP-019- V2 Fecha de vigencia: FEBRERO - 2023
---	---	---

8.2	IDENTIFICACIÓN/CUALIFICACIÓN DEL AUDITOR.....	81
8.3	RELACIÓN ENTRE EL AUDITOR Y LA AUTORIDAD AUDITADA.....	82
8.4	ASPECTOS CUBIERTOS POR LOS CONTROLES.....	82
8.5	TOMA DE DECISIONES FRENTE A LA DETECCIÓN DE DEFICIENCIAS	82
8.6	COMUNICACIÓN DE RESULTADOS	83
9.	OTROS ASPECTOS LEGALES Y DE ACTIVIDAD	83
9.1	TARIFAS	83
9.1.1	TARIFAS PARA EMISIÓN O RENOVACIÓN DE CERTIFICADO ..	83
9.1.2	TARIFAS PARA ACCESO A CERTIFICADOS	83
9.1.3	TARIFAS PARA ACCESO A INFORMACIÓN DE ESTADO O REVOCACIÓN.....	83
9.1.4	TARIFAS PARA OTROS SERVICIOS.....	84
9.1.5	POLÍTICA DE REEMBOLSO	84
9.2	RESPONSABILIDADES ECONÓMICAS.....	84
9.2.1	SEGURO DE RESPONSABILIDAD CIVIL.....	84
9.2.2	OTROS ACTIVOS	84
9.2.3	SEGUROS Y GARANTÍAS PARA ENTIDADES FINALES.....	84
9.3	CONFIDENCIALIDAD DE LA INFORMACIÓN	84
9.3.1	ALCANCE DE LA INFORMACIÓN CONFIDENCIAL.....	85
9.3.2	INFORMACIÓN NO CONFIDENCIAL.....	85
9.3.3	RESPONSABILIDAD DE PROTEGER LA INFORMACIÓN CONFIDENCIAL.....	85
9.4	PROTECCIÓN DE LA INFORMACIÓN PERSONAL	86
9.5	DERECHOS DE PROPIEDAD INTELECTUAL	86
9.6	OBLIGACIONES Y GARANTÍAS.....	86
9.6.1	OBLIGACIONES DE LAS AC	86
9.6.2	OBLIGACIONES DE LA AR.....	87
9.6.3	OBLIGACIONES DE LOS SUSCRIPTORES DE LOS CERTIFICADOS.....	88
9.6.4	OBLIGACIONES DE LOS TERCEROS QUE CONFÍAN O ACEPTEN LOS CERTIFICADOS.....	89
9.7	EXENCIÓN DE RESPONSABILIDADES.....	89
9.8	LIMITACIONES DE LAS RESPONSABILIDADES.....	90



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

SECRETARÍA GENERAL

Código:
POL-GIF-GGI-NDP-019-
V2

Fecha de vigencia:
FEBRERO - 2023

9.9	INDEMNIZACIONES	91
9.9.1	INDEMNIZACIONES DE LA AC	91
9.9.2	INDEMNIZACIONES DE LOS SUSCRIPTORES	91
9.9.3	INDEMNIZACIONES DE LAS PARTES QUE CONFÍAN	91
9.10	PERÍODO DE VALIDEZ DE ESTE DOCUMENTO	92
9.10.1	PERIODO	92
9.10.2	TERMINACIÓN DE LA DPC	92
9.10.3	EFFECTOS DE LA TERMINACIÓN	92
9.11	NOTIFICACIONES INDIVIDUALES Y COMUNICACIONES CON LOS PARTICIPANTES	92
9.12	MODIFICACIONES DE ESTE DOCUMENTO	93
9.12.1	PROCEDIMIENTO PARA LAS MODIFICACIONES	93
9.12.2	PERIODO Y MECANISMO DE NOTIFICACIÓN	93
9.12.3	CIRCUNSTANCIAS BAJO LAS CUALES DEBE CAMBIARSE UN OID	93
9.13	RESOLUCIÓN DE CONFLICTOS	93
9.14	NORMATIVA APLICABLE	94
9.15	CUMPLIMIENTO DE LA LEGISLACIÓN APLICABLE	94
9.16	ESTIPULACIONES MISCELÁNEAS	94
9.16.1	ACEPTACIÓN DE LA DPC	94
9.16.2	RESOLUCIÓN DE CONFLICTOS EN LA VÍA JUDICIAL	94
9.17	OTRAS ESTIPULACIONES	94

	POLÍTICA DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN DE INFRAESTRUCTURA DE CLAVE PÚBLICA DEL SERVICIO DE ADMINISTRACIÓN DE RENTAS DE LA REPUBLICA DE HONDURAS SECRETARÍA GENERAL	Código: POL-GIF-GGI-NDP-019-V2 Fecha de vigencia: FEBRERO - 2023
---	---	--

1. INTRODUCCIÓN

El presente documento corresponde a la Declaración de Prácticas de Certificación (DPC), que estipula el funcionamiento y operaciones de la Infraestructura de Clave Pública (en adelante PKI) del Servicio de Administración de Rentas (en adelante, el SAR) de la República de Honduras; en concordancia con las recomendaciones de la Request for Comments RFC 3647 "Internet X.509 Public Key Infrastructure: Certificate Policy and Certification Practices Framework", de 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, jurídicas, funcionarios(as) y empleados(as) públicos(as), así como a los terceros que confían en los certificados y servicios de sellado de tiempo brindados por el SAR.

1.1 Visión General

1.1.1 Control del Documento

Versión	Motivo	Fecha de vigencia	Documentos que Elimina
1.0	Creación	Diciembre 2021	N/A
2.0	Actualización de aspectos	Enero- 2023	ACUERDO NUMERO- SAR-520 -2021, Política Declaración de Prácticas de Certificación de Infraestructura de Clave Pública del Servicio de Administración de Rentas de la República De Honduras , POL-GIF-GGI-001-V1.

	POLÍTICA DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN DE INFRAESTRUCTURA DE CLAVE PÚBLICA DEL SERVICIO DE ADMINISTRACIÓN DE RENTAS DE LA REPUBLICA DE HONDURAS	Código: POL-GIF-GGI-NDP-019-V2 Fecha de vigencia: FEBRERO - 2023
SECRETARÍA GENERAL		

1.1.2 Objetivo 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

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 recoge las Políticas de Certificación, las cuales regirán el funcionamiento y operaciones de la Infraestructura de Clave Pública del Servicio de Administración de Rentas de Honduras (PKI-SAR).

	POLÍTICA DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN DE INFRAESTRUCTURA DE CLAVE PÚBLICA DEL SERVICIO DE ADMINISTRACIÓN DE RENTAS DE LA REPUBLICA DE HONDURAS SECRETARÍA GENERAL	Código: POL-GIF-GGI-NDP-019- V2 Fecha de vigencia: FEBRERO - 2023
---	---	---

1.1.6 Alcance

La totalidad de los certificados emitidos por la PKI-SAR cumplen con lo estipulado en la versión 2 del estándar RFC 3647. De esta manera, se hace posible la adición de extensiones para la certificación de atributos.

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 prevalecerán 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 DPC 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 con base en las recomendaciones de la RFC 3647 (Plantilla de Declaración de Prácticas de Certificación de Llave Pública), a fin de hacer de fácil comprensión para el lector. Existen secciones las cuales determinamos como "No Estipulado": dichas secciones del documento no tienen inherencia en nuestro marco de cumplimiento.

	POLÍTICA DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN DE INFRAESTRUCTURA DE CLAVE PÚBLICA DEL SERVICIO DE ADMINISTRACIÓN DE RENTAS DE LA REPUBLICA DE HONDURAS SECRETARÍA GENERAL	Código: POL-GIF-GGI-NDP-019- V2 Fecha de vigencia: FEBRERO - 2023
---	---	---

1.1.9 Marco Normativo

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

1.1.10 Referencia Técnica

<i>Documentos de Referencia</i>	<i>Fecha de vigencia</i>
Recomendaciones del RFC 2560	1999
Recomendaciones del RFC 3161 – TSA	2001
Recomendaciones del RFC 3647 – PC	2003
Versión 3 del estándar X.509	2008
Recomendaciones del RFC 5280 – CRL	2008
Recomendaciones del RFC 6960 – OSCP	2013
ISO/IEC 27001 – Sistema de gestión de seguridad	2018

1.2 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 2** y será vigente a partir de su fecha de 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/>

	POLÍTICA DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN DE INFRAESTRUCTURA DE CLAVE PÚBLICA DEL SERVICIO DE ADMINISTRACIÓN DE RENTAS DE LA REPUBLICA DE HONDURAS SECRETARÍA GENERAL	Código: POL-GIF-GGI-NDP-019- V2 Fecha de vigencia: FEBRERO - 2023
---	---	---

El Identificador de Objetos (OID) correspondiente a este documento es el siguiente:
1.3.6.1.4.1.52089.2.1

1.3 Participantes de la PKI-SAR

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

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

La jerarquía de confianza de la PKI-SAR, es la siguiente:

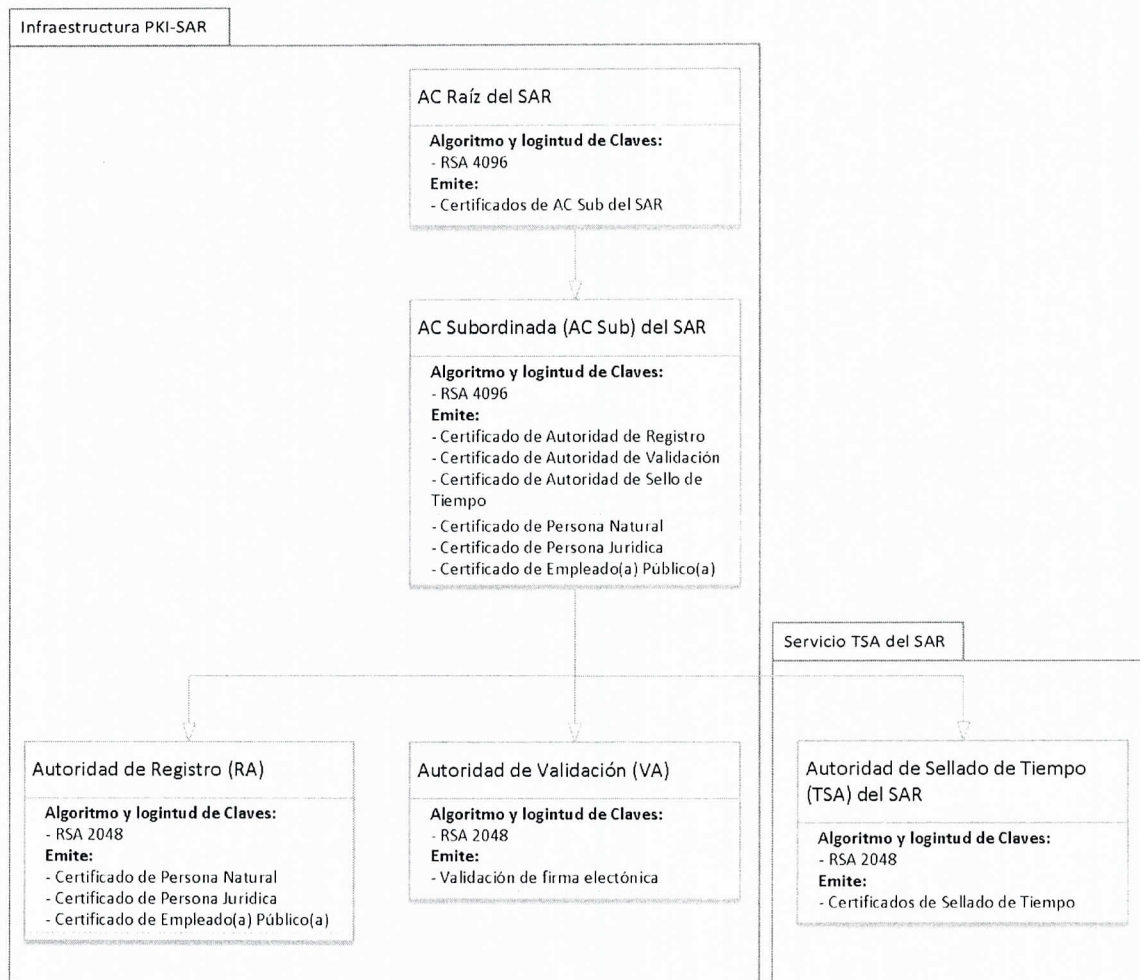


**POLÍTICA DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN
DE INFRAESTRUCTURA DE CLAVE PÚBLICA DEL SERVICIO DE
ADMINISTRACIÓN DE RENTAS DE LA REPUBLICA DE
HONDURAS**

SECRETARÍA GENERAL

Código:
POL-GIF-GGI-NDP-019-
V2

Fecha de vigencia:
FEBRERO - 2023



1.3.1 Autoridad 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).

	POLÍTICA DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN DE INFRAESTRUCTURA DE CLAVE PÚBLICA DEL SERVICIO DE ADMINISTRACIÓN DE RENTAS DE LA REPUBLICA DE HONDURAS SECRETARÍA GENERAL	Código: POL-GIF-GGI-NDP-019- V2 Fecha de vigencia: FEBRERO - 2023
---	---	---

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 Autoridad Certificadora Raíz del SAR es la designada para la emisión del certificado Raíz regida bajo la presente DPC. El certificado Raíz consiste en un certificado auto firmado que se encuentra fuera de línea, mediante el cual se inicia la cadena de confianza; este debe permanecer offline una vez se realice la ceremonia de llaves y se generen los certificados subordinados necesarios. Su encendido como apagado obedece a un procedimiento realizado para esta actividad.

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

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

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

	POLÍTICA DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN DE INFRAESTRUCTURA DE CLAVE PÚBLICA DEL SERVICIO DE ADMINISTRACIÓN DE RENTAS DE LA REPUBLICA DE HONDURAS SECRETARÍA GENERAL	Código: POL-GIF-GGI-NDP-019-V2 Fecha de vigencia: FEBRERO - 2023
---	---	--

Contenido del certificado Autoridad Certificadora Raíz del SAR				
Nombre	Atributo	Valor	Obligatorio	Crítica
	Not Before	2043-02-28 12:25:20	Si	-
Subject	CN	AUTORIDAD CERTIFICADORA RAIZ DEL SAR	Si	-
	O	SERVICIO DE ADMINISTRACION DE RENTAS	Si	-
	C	HN	Si	-
Subject Public Key Info	Algorithm	RSA	Si	-

1.3.3 Autoridad Certificadora Subordinada del SAR

La Autoridad Certificadora Subordinada del SAR es la designada para la emisión del certificado Subordinado regido bajo la presente DPC. Este certificado es el siguiente en jerarquía a la Autoridad Certificación Raíz; por tanto, la AC Subordinada es la encargada de la emisión de todos los certificados finales para persona natural, persona jurídica o funcionarios(as) y/o empleados(as) públicos(as).

En la siguiente tabla se detallan los datos con más relevancia de la Autoridad Subordinada 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 ADMINISTRACION DE RENTAS	Si	-

	POLÍTICA DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN DE INFRAESTRUCTURA DE CLAVE PÚBLICA DEL SERVICIO DE ADMINISTRACIÓN DE RENTAS DE LA REPUBLICA DE HONDURAS SECRETARÍA GENERAL	Código: POL-GIF-GGI-NDP-019-V2 Fecha de vigencia: FEBRERO - 2023
---	---	--

Contenido del certificado Autoridad Subordinada del SAR				
Nombre	Atributo	Valor	Obligatorio	Crítica
	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 ADMINISTRACION 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 esta DPC y las PC.

La PKI-SAR 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.

1.3.5 Autoridad de Validación (AV)

La Autoridad de Validación (AV) es la entidad que determina de forma online el estado actual de cualquier certificado emitido por el componente Autoridad

	POLÍTICA DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN DE INFRAESTRUCTURA DE CLAVE PÚBLICA DEL SERVICIO DE ADMINISTRACIÓN DE RENTAS DE LA REPUBLICA DE HONDURAS SECRETARÍA GENERAL	Código: POL-GIF-GGI-NDP-019-V2 Fecha de vigencia: FEBRERO - 2023
---	---	--

Certificación Subordinada, a través del protocolo OCSP, de acuerdo con los estándares RFC 6960 y RFC2560. dispuestos en la URL http://ocsp.sar.gob.hn/CryptosecOpenKey/va_service Las respuestas OCSP emitidas están firmadas con la clave privada correspondiente al certificado de firma de respuestas OCSP del componente AV.

El mecanismo antes mencionado, es complementario al proceso de publicación de las Listas de Certificados Revocados (CRL), de acuerdo con el estándar RFC 5280 dispuesto en la URL <http://pki.sar.gob.hn/crlsar/crl.crl>

1.3.6 Autoridad de Sellado de Tiempo (AST)

La Autoridad de Sellado de Tiempo (AST) es la entidad responsable de probar que un conjunto de datos existió antes de un momento dado y que ninguno de estos datos ha sido modificado desde entonces. El sellado de tiempo provee un valor añadido a la utilización de Firma Electrónica, ya que ésta por sí sola no proporciona ninguna información acerca del momento de creación de la firma y, en el caso de que el firmante la incluyese, ésta habría sido proporcionada por una de las partes. Sin embargo, lo recomendable es que la marca de tiempo sea proporcionada por una tercera parte de confianza de acuerdo con el estándar RFC3161.

1.3.7 Solicitantes y Suscriptores de Certificados

Los solicitantes de certificados son definidos por la DPC de la PKI-SAR. Dentro del contexto de esta DPC, los suscriptores y solicitantes de “Certificado de Firma Electrónica” son cualquier persona natural que posea un 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, una persona jurídica debidamente registrada en el territorio nacional y un(a) empleado(a) público(a) con la documentación que acredite que ostenta un cargo en la Administración Pública.

	POLÍTICA DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN DE INFRAESTRUCTURA DE CLAVE PÚBLICA DEL SERVICIO DE ADMINISTRACIÓN DE RENTAS DE LA REPUBLICA DE HONDURAS SECRETARÍA GENERAL	Código: POL-GIF-GGI-NDP-019- V2 Fecha de vigencia: FEBRERO - 2023
---	---	---

1.3.8 Terceros que confían en los certificados emitidos por la PKI-SAR

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

1.3.9 Autoridad Administrativa Competente (AAC)

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

1.3.10 Prestador de Servicios de Certificación (PSC)

La autoridad certificadora o Prestador de Servicios de Certificación PSC, autorizados por la AAC pueden realizar, entre otras, las siguientes actividades:

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

	POLÍTICA DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN DE INFRAESTRUCTURA DE CLAVE PÚBLICA DEL SERVICIO DE ADMINISTRACIÓN DE RENTAS DE LA REPUBLICA DE HONDURAS SECRETARÍA GENERAL	Código: POL-GIF-GGI-NDP-019- V2 Fecha de vigencia: FEBRERO - 2023
---	---	---

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 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 AAC; 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 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 debe 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.

	POLÍTICA DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN DE INFRAESTRUCTURA DE CLAVE PÚBLICA DEL SERVICIO DE ADMINISTRACIÓN DE RENTAS DE LA REPUBLICA DE HONDURAS SECRETARÍA GENERAL	Código: POL-GIF-GGI-NDP-019- V2 Fecha de vigencia: FEBRERO - 2023
---	---	---

- 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 del certificado se determina por medio de las PC correspondientes a cada tipo de certificado.

1.4.2 Prohibiciones de Uso de los Certificados.

Los certificados deben ser empleados para los usos detallados explícitamente en las PC correspondiente, y se prohíbe su uso para cualquier actividad o fines no contemplados en dichos documentos.

	POLÍTICA DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN DE INFRAESTRUCTURA DE CLAVE PÚBLICA DEL SERVICIO DE ADMINISTRACIÓN DE RENTAS DE LA REPUBLICA DE HONDURAS SECRETARÍA GENERAL	Código: POL-GIF-GGI-NDP-019- V2 Fecha de vigencia: FEBRERO - 2023
---	---	---

1.5 Administración de las Políticas

1.5.1 Organización Responsable de la DPC

Los términos y redacción de la presente DPC de PKI-SAR son establecidos por el Servicio de Administración de Rentas a través de su Comité de Firma Electrónica, quien es la entidad responsable también de realizar revisiones periódicas a las mismas, de manera que se mantengan actualizadas.

1.5.2 Procedimiento de Aprobación y Modificación de la DPC

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

1.5.3 Responsable por Modificaciones a la DPC

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

Todas las modificaciones realizadas a la DPC deben ser publicadas en el sitio web del 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 dará derecho al Suscriptor de recibir compensación por este motivo.

	POLÍTICA DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN DE INFRAESTRUCTURA DE CLAVE PÚBLICA DEL SERVICIO DE ADMINISTRACIÓN DE RENTAS DE LA REPUBLICA DE HONDURAS SECRETARÍA GENERAL	Código: POL-GIF-GGI-NDP-019- V2 Fecha de vigencia: FEBRERO - 2023
---	---	---

1.5.4 Datos de Contacto

Nombre de Entidad: Servicio de Administración de Rentas - SAR

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

Correo: pki@sar.gob.hn

Teléfono: (504) 2216-5800

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

	POLÍTICA DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN DE INFRAESTRUCTURA DE CLAVE PÚBLICA DEL SERVICIO DE ADMINISTRACIÓN DE RENTAS DE LA REPUBLICA DE HONDURAS SECRETARÍA GENERAL	Código: POL-GIF-GGI-NDP-019- V2 Fecha de vigencia: FEBRERO - 2023
---	---	---

1.6 Glosario y Siglas

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.
- Ceremonia de Llaves:** Es la puesta en marcha de los elementos hardware y software de una AC en el entorno de producción de la infraestructura que es utilizada por PKI-SAR para prestar servicios de certificación, garantizando la seguridad en la generación de las claves del certificado de la AC y en el posterior uso de su correspondiente clave privada.
- Certificado Electrónico:** Todo mensaje de datos proporcionado por un “Prestador de Servicios de Certificación” que le atribuye certeza y validez a la Firma Electrónica.
- Certificado Subordinado:** Es el certificado emitido por la AC para autoridades intermedias, garantizando que el propietario del certificado es quien dice ser.
- Clave Privada:** Componente confidencial del Suscriptor, utilizado para el proceso de cifrado o firmado electrónico.



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

SECRETARÍA GENERAL

Código:
POL-GIF-GGI-NDP-019-
V2

Fecha de vigencia:
FEBRERO - 2023

- **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 sí mismos y frente a terceros.
- **Persona Natural:** Individuo debidamente identificado en el territorio de la República de Honduras, mediante su Documento Nacional de Identificación.

	POLÍTICA DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN DE INFRAESTRUCTURA DE CLAVE PÚBLICA DEL SERVICIO DE ADMINISTRACIÓN DE RENTAS DE LA REPUBLICA DE HONDURAS SECRETARÍA GENERAL	Código: POL-GIF-GGI-NDP-019- V2 Fecha de vigencia: FEBRERO - 2023
---	---	---

- Prestador de Servicios de Certificación:** Un Prestador de Servicios de Certificación es una persona, física o jurídica, que expide certificados electrónicos o que presta otros servicios en relación con la Firma Electrónica.
- Repositorio Criptográfico de Software PKCS12:** Archivo para el almacenamiento de muchos objetos criptográficos en un solo archivo.
- Repositorios:** Archivo es un sitio centralizado donde se almacena y mantiene información digital de los CRL, certificados, DPC y PC.
- Revocación:** La revocación de un certificado se define por la acción mediante la cual se invalida un certificado antes de su fecha de caducidad.
- Solicitante:** Individuo que solicita un certificado electrónico mediante los procesos provistos por la PKI-SAR.
- Suscriptor:** 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.



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

SECRETARÍA GENERAL

Código:
POL-GIF-GGI-NDP-019-
V2

Fecha de vigencia:
FEBRERO - 2023

- **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.

	POLÍTICA DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN DE INFRAESTRUCTURA DE CLAVE PÚBLICA DEL SERVICIO DE ADMINISTRACIÓN DE RENTAS DE LA REPUBLICA DE HONDURAS SECRETARÍA GENERAL	Código: POL-GIF-GGI-NDP-019- V2 Fecha de vigencia: FEBRERO - 2023
---	---	---

1.6.2 Siglas

- **AAC:** Autoridad Administrativa Competente.
- **AC:** Autoridad de Certificación.
- **AR:** Autoridad de Registro.
- **ARL** Authority Revocation List - Lista de Revocación de Autoridad.
- **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:** Módulo Criptográfico de Seguridad o Hardware Security Module por siglas en Inglés. 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.



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

SECRETARÍA GENERAL

Código:
POL-GIF-GGI-NDP-019-
V2

Fecha de vigencia:
FEBRERO - 2023

- **OID:** Object Identifier - Identificador Único de Objeto.
- **OU:** Organizational Unit - Unidad Organizacional. Correspondiente a estándar X.500.
- **PC:** Política de Certificación.
- **PIN:** Personal Identification 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:** Estándares que establecen los requisitos para PKI por Internet Engineering Task Force.
- **PKI-SAR:** Infraestructura de Clave Pública del Servicio de Administración de Rentas.
- **ST:** State - Estado. Correspondiente a estándar x.500.

	POLÍTICA DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN DE INFRAESTRUCTURA DE CLAVE PÚBLICA DEL SERVICIO DE ADMINISTRACIÓN DE RENTAS DE LA REPUBLICA DE HONDURAS SECRETARÍA GENERAL	Código: POL-GIF-GGI-NDP-019- V2 Fecha de vigencia: FEBRERO - 2023
---	---	---

2. REPOSITORIOS Y PUBLICACIÓN DE INFORMACIÓN

2.1 Repositorios

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

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

2.2 Publicación de Información de Certificación

Como parte de las obligaciones y responsabilidades de las AC pertenecientes a la Jerarquía de confianza de la PKI-SAR, 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, al que se hace mención en el numeral 2.1 Repositorios.

Las PC son de carácter público y se encuentran publicadas en el sitio web de SAR, al que se hace mención en el numeral 2.1. Repositorios.

Las listas de revocación de certificados CRL son de carácter público y se encuentran publicadas en el servidor web de PKI-SAR, al que se hace mención en el numeral 2.1 Repositorios.

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

	POLÍTICA DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN DE INFRAESTRUCTURA DE CLAVE PÚBLICA DEL SERVICIO DE ADMINISTRACIÓN DE RENTAS DE LA REPUBLICA DE HONDURAS SECRETARÍA GENERAL	Código: POL-GIF-GGI-NDP-019- V2 Fecha de vigencia: FEBRERO - 2023
---	---	---

2.3 Tiempos y Frecuencia de Publicación

La DPC, será publicada consecuentemente al momento de su aprobación. Dicha documentación será publicada en el sitio web al que se hace mención en el numeral 2.1 Repositorios.

La AC agregará los certificados que hayan sido revocados a la CRL correspondiente, la ventana de tiempo debe ser acorde al punto 4.9.7 frecuencia de emisión de CRL.

2.4 Controles de Acceso a los Repositorios

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 el SAR. Por tal motivo, este último es responsable de establecer los controles necesarios para que personas no autorizadas no puedan manipular la información que reposa en dichos repositorios.

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 Public Key Infrastructure Certificate and Certificate Revocation List CRL".

El proceso para realizar la asignación de los Nombres Distintivos (DN) para cada uno de los Suscriptores basándonos en el tipo de certificado es definido por la PC correspondiente a cada tipo de certificado. Las PC antes mencionadas deben ser acordes a las directrices descritas en esta DPC.

	POLÍTICA DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN DE INFRAESTRUCTURA DE CLAVE PÚBLICA DEL SERVICIO DE ADMINISTRACIÓN DE RENTAS DE LA REPUBLICA DE HONDURAS SECRETARÍA GENERAL	Código: POL-GIF-GGI-NDP-019- V2 Fecha de vigencia: FEBRERO - 2023
---	---	---

3.1.2 Necesidad de que los Nombres sean Significativos

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

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

3.1.3 Regla para Interpretar varios formatos de nombres

La PKI-SAR 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.

3.1.4 Unicidad de los Nombres

La agrupación del Nombre Distintivo (DN) más el contenido de la extensión *Policy Identifier* 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 PC correspondiente.

3.1.5 Reconocimiento, autenticación y papel de las marcas registradas

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

	POLÍTICA DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN DE INFRAESTRUCTURA DE CLAVE PÚBLICA DEL SERVICIO DE ADMINISTRACIÓN DE RENTAS DE LA REPUBLICA DE HONDURAS SECRETARÍA GENERAL	Código: POL-GIF-GGI-NDP-019- V2 Fecha de vigencia: FEBRERO - 2023
---	---	---

3.2 Validación Inicial de Identidad

3.2.1 Métodos para comprobar la clave privada

La PC aplicable a cada tipo de certificado define el procedimiento de comprobación de la clave privada.

3.2.2 Autenticación de la identidad de la organización

La PC aplicable a cada tipo de certificado define el procedimiento de comprobación de la clave privada.

3.2.3 Autenticación de la identidad de la persona física solicitante

La PC aplicable a cada tipo de certificado define el procedimiento de comprobación de la clave privada.

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

La PC aplicable a cada tipo de certificado definirá el procedimiento de comprobación de la clave privada.

3.2.6 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 el país si presenta un grado de fiabilidad equivalente.

	POLÍTICA DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN DE INFRAESTRUCTURA DE CLAVE PÚBLICA DEL SERVICIO DE ADMINISTRACIÓN DE RENTAS DE LA REPUBLICA DE HONDURAS SECRETARÍA GENERAL	Código: POL-GIF-GGI-NDP-019- V2 Fecha de vigencia: FEBRERO - 2023
---	---	---

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 Artículo 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.

3.3 Identificación y autenticación para solicitudes de renovación

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

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

4.1 Solicitud de certificados

El procedimiento establecido para la emisión de certificados de Firma Electrónica está establecido en la PC correspondiente.

4.1.1 ¿Quien puede realizar una solicitud?

Las PC 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. Dichas PC deben detallar los pasos que deben seguirse para completar este proceso.

	POLÍTICA DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN DE INFRAESTRUCTURA DE CLAVE PÚBLICA DEL SERVICIO DE ADMINISTRACIÓN DE RENTAS DE LA REPUBLICA DE HONDURAS SECRETARÍA GENERAL	Código: POL-GIF-GGI-NDP-019- V2 Fecha de vigencia: FEBRERO - 2023
---	---	---

4.1.2 Proceso de enrolamiento y responsabilidades de los solicitantes

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

Los solicitantes son los 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 PC correspondiente a cada caso.

4.2 Gestión de las solicitudes de certificados

4.2.1 Funciones de identificación y autenticación

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

4.2.2 Rechazo o Aceptación de solicitudes de certificado

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

La AR de 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;
- Si la información concerniente a identificación y autenticación de toda la información requerida en cada PC no puede ser completada;
- 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;

	POLÍTICA DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN DE INFRAESTRUCTURA DE CLAVE PÚBLICA DEL SERVICIO DE ADMINISTRACIÓN DE RENTAS DE LA REPUBLICA DE HONDURAS SECRETARÍA GENERAL	Código: POL-GIF-GGI-NDP-019- V2 Fecha de vigencia: FEBRERO - 2023
---	---	---

- Por otros casos justificados, dependiendo de la particularidad de la documentación solicitada para cada tipo certificado, las que se estipularán en cada una de las PC correspondientes;

4.2.3 Plazo para la gestión de las solicitudes

La AR de la PKI-SAR no se hará responsable por retrasos que puedan surgir entre la solicitud del certificado y la entrega de este. En cualquier caso, el plazo para la tramitación de las solicitudes de certificados estará condicionada a la disponibilidad de citas en las oficinas de registros, a la que desee acudir el solicitante.

4.3 Emisión de Certificados

4.3.1 Acciones de la AC durante la emisión de certificado.

La acción de emitir un certificado implica la autorización definitiva de la solicitud de certificación por parte de la AC. Al momento de la emisión del certificado en base a la solicitud, se realizarán las notificaciones que se describen el numeral 4.7.7 denominado notificación de la emisión del certificado por la AC a otras Autoridades.

La vigencia de los certificados inicia al momento de emisión de estos. 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.

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

4.3.2 Notificación al solicitante de la emisión por la AC del certificado

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

	POLÍTICA DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN DE INFRAESTRUCTURA DE CLAVE PÚBLICA DEL SERVICIO DE ADMINISTRACIÓN DE RENTAS DE LA REPUBLICA DE HONDURAS SECRETARÍA GENERAL	Código: POL-GIF-GGI-NDP-019- V2 Fecha de vigencia: FEBRERO - 2023
---	---	---

4.4 Aceptación del certificado

4.4.1 Acción que afirma la aceptación del certificado

El proceso de aceptación del certificado se encuentra estipulado por la PC correspondiente a cada tipo de certificado.

4.4.2 Publicación del certificado por parte de la AC

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

4.4.3 Notificación de la emisión del certificado por la AC a otras entidades

No se realizan notificaciones de emisión a otras entidades.

4.5 Uso del Par de Claves y certificado

4.5.1 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, son definidas en los términos y condiciones correspondiente a cada caso. De cualquier forma, el Suscriptor solo puede emplear el certificado y la clave privada para los usos descritos en las PC 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 PC correspondiente.

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

	POLÍTICA DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN DE INFRAESTRUCTURA DE CLAVE PÚBLICA DEL SERVICIO DE ADMINISTRACIÓN DE RENTAS DE LA REPUBLICA DE HONDURAS SECRETARÍA GENERAL	Código: POL-GIF-GGI-NDP-019- V2 Fecha de vigencia: FEBRERO - 2023
---	---	---

4.5.2 Uso de la clave pública y del certificado por lo terceros que confían.

Los terceros deben confiar únicamente en los certificados para 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.

4.6 Renovación de certificados sin cambio de clave

4.6.1 Circunstancias para la renovación de certificados sin cambio de clave ausente

La totalidad de las renovaciones de certificados llevadas a cabo bajo el ámbito de la presente DPC, serán con cambio de claves. Por lo tanto, los puntos referentes a la renovación de certificados sin cambios de clave (puntos 4.6.3, 4.6.4, 4.6.5, 4.6.6 4.6.7 y 4.6.7), los cuales son establecidos en el RFC 7382; en consecuencia, a efectos de esta DPC, su no estipulación.

4.6.2 Gestión de las peticiones de renovación de certificados sin cambio de claves

No estipulado



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

SECRETARÍA GENERAL

Código:
POL-GIF-GGI-NDP-019-
V2

Fecha de vigencia:
FEBRERO - 2023

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 ausente

No estipulado

4.6.6 Publicación del certificado sin cambio de clave ausente

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

4.7.1 Circunstancias para la Renovación con Cambio de Claves de un Certificado

No estipulado.

	POLÍTICA DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN DE INFRAESTRUCTURA DE CLAVE PÚBLICA DEL SERVICIO DE ADMINISTRACIÓN DE RENTAS DE LA REPUBLICA DE HONDURAS SECRETARÍA GENERAL	Código: POL-GIF-GGI-NDP-019- V2 Fecha de vigencia: FEBRERO - 2023
---	---	---

4.7.2 Quién puede pedir la renovación de los certificados

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

4.7.3 Gestión de las peticiones de renovación de certificados con cambio de claves

La PC 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 tiempo y forma, de acuerdo con las instrucciones y normativa establecidas por la PKI-SAR para este propósito.
- Que la AC 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 para el mismo tipo de certificado emitido en primera instancia.

4.7.4 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.

4.7.5 Método de Aceptación del Certificado con Cambio de Claves

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

	POLÍTICA DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN DE INFRAESTRUCTURA DE CLAVE PÚBLICA DEL SERVICIO DE ADMINISTRACIÓN DE RENTAS DE LA REPUBLICA DE HONDURAS SECRETARÍA GENERAL	Código: POL-GIF-GGI-NDP-019- V2 Fecha de vigencia: FEBRERO - 2023
---	---	---

4.7.6 Publicación del certificado con las nuevas claves por parte de la AC

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

4.7.7 Notificación de la Emisión del Certificado por la AC a otras Autoridades

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

4.8 Modificación de certificados

No es posible realizar modificaciones a los certificados expedidos. Por tanto, cualquier necesidad de modificación conlleva la expedición de un nuevo certificado.

Consecuentemente, el resto de los puntos 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 y 4.8.7) no son estipulados 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.

	POLÍTICA DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN DE INFRAESTRUCTURA DE CLAVE PÚBLICA DEL SERVICIO DE ADMINISTRACIÓN DE RENTAS DE LA REPUBLICA DE HONDURAS SECRETARÍA GENERAL	Código: POL-GIF-GGI-NDP-019- V2 Fecha de vigencia: FEBRERO - 2023
---	---	---

4.8.5 Método de aceptación del certificado modificado

No estipulado.

4.8.6 Publicación del certificado modificado por la CA

No estipulado.

4.8.7 Notificación de la modificación del certificado por la CA a otras entidades

No estipulado.

4.9 Revocación y suspensión de certificados

4.9.1 Circunstancias para la revocación

La revocación de un certificado se define por la acción mediante la cual se invalida un certificado antes de su fecha de caducidad.

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

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

- Por pérdida 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



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

SECRETARÍA GENERAL

Código:
POL-GIF-GGI-NDP-019-
V2

Fecha de vigencia:
FEBRERO - 2023

podrá ser revocado:

- A petición del Suscriptor o un tercero en su nombre y representación debidamente facultado.
- 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 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 la AAC.
- Por declaración de insolvencia, siempre que, en el plazo fijado por ley, no se levante dicho estado.
- Cualquier otra causa lícita prevista en la declaración de prácticas de certificación.

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

4.9.2 ¿Quién puede solicitar la Revocación?

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

La revocación también puede ser solicitada por el Suscriptor o sus responsables, acogiéndose a las condiciones descritas en el numeral 4.9.3 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, 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 sea revocado.

	POLÍTICA DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN DE INFRAESTRUCTURA DE CLAVE PÚBLICA DEL SERVICIO DE ADMINISTRACIÓN DE RENTAS DE LA REPUBLICA DE HONDURAS SECRETARÍA GENERAL	Código: POL-GIF-GGI-NDP-019- V2 Fecha de vigencia: FEBRERO - 2023
---	---	---

Las PC podrían definir políticas o procedimientos más estrictos.

4.9.3 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 éste mediante correo electrónico.
- Posterior a la revocación del certificado, el Suscriptor debe suspender el uso de la clave privada que 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 PC especificará la información necesaria para realizar la solicitud de revocación de un certificado.

4.9.4 Periodo en que se 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.

4.9.5 Plazo en el que se debe resolver la solicitud de revocación

Las PC 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, desde la recepción de la solicitud de revocación en días laborables y nunca superior a 72 horas en días no laborables.

	POLÍTICA DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN DE INFRAESTRUCTURA DE CLAVE PÚBLICA DEL SERVICIO DE ADMINISTRACIÓN DE RENTAS DE LA REPUBLICA DE HONDURAS SECRETARÍA GENERAL	Código: POL-GIF-GGI-NDP-019- V2 Fecha de vigencia: FEBRERO - 2023
---	---	---

4.9.6 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 AV mediante el protocolo OCSP para verificar las revocaciones, en caso de no disponibilidad de este servicio, deben consultar las CRL dispuestas de manera pública descritas en el numeral 2.1 Repositorios, 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 P C.

4.9.7 Frecuencia de emisión de CRL

Los métodos de verificación serán mediante el protocolo OCSP y mediante las CRL. La PKI-SAR publicará una nueva CRL en su repositorio correspondiente al momento en que se realice cualquier revocación. No obstante, la PKI-SAR publicará una nueva CRL en el repositorio correspondiente en espacios de tiempo no mayores a 24 horas para las ACS. Para el caso de la ARL de la ACR, debe realizarse la publicación de esta al instante en que se efectúe la revocación del Certificado de la ACS, el intervalo de publicación de una nueva ARL no debe ser superior a un (1) año en caso en que haya o no revocaciones.

4.9.8 Tiempo máximo entre la generación y la publicación de las CRL

Las PC correspondientes a cada tipo de certificado establecerán el período de tiempo máximo aceptable, entre la generación y publicación de las CRL en su repositorio. Sin embargo, para el caso de la AR de la ACR, debe realizarse la publicación de esta al instante en que se efectúe la revocación del Certificado de la ACS.

	POLÍTICA DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN DE INFRAESTRUCTURA DE CLAVE PÚBLICA DEL SERVICIO DE ADMINISTRACIÓN DE RENTAS DE LA REPUBLICA DE HONDURAS SECRETARÍA GENERAL	Código: POL-GIF-GGI-NDP-019- V2 Fecha de vigencia: FEBRERO - 2023
---	---	---

4.9.9 Disponibilidad de un sistema en línea de verificación del estado de los certificados

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

4.9.10 Requisitos de comprobación en línea de revocación

Con el fin de ser capaz de interactuar con la AV, 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.

4.9.11 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.

4.9.12 Causas para la suspensión

La suspensión de la vigencia de los certificados (en el caso de que dicha operación esté contemplada por la PC correspondiente) se aplicará, 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 PC.
- 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.



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

SECRETARÍA GENERAL

Código:
POL-GIF-GGI-NDP-019-
V2

Fecha de vigencia:
FEBRERO - 2023

- 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 empleado(a) público(a).
- Las demás causales que establezcan en sus respectivas PC.

4.9.13 Quién puede solicitar la suspensión

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

4.9.14 Procedimiento para la Solicitud de Suspensión

Cada PC establecerá el procedimiento para la solicitud de suspensión.

4.9.15 Límites del periodo de suspensión

Sin perjuicio de lo definido en las PC, 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.

4.10 Servicios de información del estado de certificados

4.10.1 Características operativas

La PKI-SAR 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 AC:

	POLÍTICA DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN DE INFRAESTRUCTURA DE CLAVE PÚBLICA DEL SERVICIO DE ADMINISTRACIÓN DE RENTAS DE LA REPUBLICA DE HONDURAS SECRETARÍA GENERAL	Código: POL-GIF-GGI-NDP-019- V2 Fecha de vigencia: FEBRERO - 2023
---	---	---

- La AV 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.

4.10.2 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.

4.10.3 Características Adicionales

La PKI-SAR 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.

4.11 Finalización de la validez de un certificado

La suscripción finalizará en el momento de extinción de la vigencia del Certificado, ya sea por expiración del periodo de vigencia o por revocación de este. De no llevarse a cabo la renovación del certificado, se considerará extinguida la relación entre el dueño del certificado y la PKI-SAR.

	POLÍTICA DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN DE INFRAESTRUCTURA DE CLAVE PÚBLICA DEL SERVICIO DE ADMINISTRACIÓN DE RENTAS DE LA REPUBLICA DE HONDURAS SECRETARÍA GENERAL	Código: POL-GIF-GGI-NDP-019- V2 Fecha de vigencia: FEBRERO - 2023
---	---	---

4.12 Custodia y recuperación de claves

4.12.1 Prácticas y políticas de recuperación de claves

La PKI-SAR no recuperará las claves privadas asociadas a los certificados.

4.12.2 Prácticas y políticas de recuperación de claves de sesión

No estipulado.

5. CONTROLES DE INSTALACIONES, GESTIÓN Y OPERACIONALES

El SAR dispone de un sistema de monitoreo y registro de eventos, este sistema funciona 24/7, recolectando en todo momento información y eventos de seguridad de todos los elementos sensibles y de confianza de la PKI-SAR para su posterior procesamiento y correlación

Los sistemas e infraestructura empleados para las operaciones del servicio de certificados digitales se encuentran administrados en el Centro de Datos del SAR, el cual cumple con los estándares de los ISO 27001 y TIER II.

5.1 Controles físicos

5.1.1 Ubicación física y construcción

La infraestructura tecnológica de la PKI-SAR 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-SAR, deben disponer como mínimo de los siguientes aspectos de seguridad física:

- Sistema interrumpible de energía (UPS).
- Sistema de UPS redundante.

	POLÍTICA DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN DE INFRAESTRUCTURA DE CLAVE PÚBLICA DEL SERVICIO DE ADMINISTRACIÓN DE RENTAS DE LA REPUBLICA DE HONDURAS SECRETARÍA GENERAL	Código: POL-GIF-GGI-NDP-019- V2 Fecha de vigencia: FEBRERO - 2023
---	---	---

- 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.

5.1.2 Acceso físico

La infraestructura de la PKI-SAR 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

5.1.3 Electricidad y Acondicionador de Aires

Suministro eléctrico:

- PDU redundante.
- UPS Redundante: Sistema Ininterrumpido de Energía.
- Aire acondicionado: Sistema de enfriamiento de Aire de precisión.

5.1.4 Exposición al agua

Sistemas de drenaje y piso elevado.



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

SECRETARÍA GENERAL

Código:
POL-GIF-GGI-NDP-019-
V2

Fecha de vigencia:
FEBRERO - 2023

5.1.5 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 automáticos para la detección y extinción de estos.

5.1.6 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.

5.1.7 Manejo de residuos

La política 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.

5.1.8 Copia de seguridad fuera de las instalaciones

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

5.2 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 PKI-SAR 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 auditorías 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.

	POLÍTICA DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN DE INFRAESTRUCTURA DE CLAVE PÚBLICA DEL SERVICIO DE ADMINISTRACIÓN DE RENTAS DE LA REPUBLICA DE HONDURAS SECRETARÍA GENERAL	Código: POL-GIF-GGI-NDP-019- V2 Fecha de vigencia: FEBRERO - 2023
---	---	---

5.2.1 Roles de PKI-SAR

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

5.2.1.1 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.

5.2.1.2 Roles de gestión de la PKI-SAR

- **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 auditoría sobre los archivos, logs y trazas de los componentes informáticos de la PKI.



5.2.2 Número de personas requeridas por tarea

Será requisito asignar a un mínimo de dos personas para realizar operaciones sobre la PKI-SAR; sin embargo, las tareas del rol Operador de Certificado podrán ser realizadas por un miembro del equipo.

5.2.3 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(a) y/o empleado(a) perteneciente a un grupo no debe ser asignado a tareas de su contraparte.

5.3 Controles de personal

5.3.1 Aptitud, conocimiento y acreditación de profesionales

El talento humano designado a labores de confianza en la PKI-SAR, 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 y certificados electrónicos.
- Adiestramiento específico para la función que desempeña.
- Título académico o experiencia equivalente.

5.3.2 Proceso para comprobación de antecedentes

El Servicio de Administración de Rentas es la entidad responsable de establecer los procesos para la verificación de la experiencia y aptitudes del talento humano designado a tareas de confianza, a través de la Dirección Nacional de Talento Humano. En especial se debe verificar:

- Empleos anteriores.
- Título académico y cursos o certificaciones obtenidas.

	POLÍTICA DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN DE INFRAESTRUCTURA DE CLAVE PÚBLICA DEL SERVICIO DE ADMINISTRACIÓN DE RENTAS DE LA REPUBLICA DE HONDURAS SECRETARÍA GENERAL	Código: POL-GIF-GGI-NDP-019- V2 Fecha de vigencia: FEBRERO - 2023
---	---	---

- Comprobación de conocimientos específicos.

5.3.3 Requerimientos de Formación

El talento humano del SAR debe estar en constante formación específica. La misma debe ser estipulada en un plan anual de formación, el cual debe incluir lo siguiente:

- Definiciones y Conceptos básicos de PKI.
- Medidas de seguridad de acceso a los sistemas.
- Medidas de seguridad física de la operación.
- Tipos de servicios prestados por la AC.
- 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.

5.3.4 Requerimientos y frecuencia de reentrenamiento

El talento humano del SAR debe estar en constante actualización de su currículum 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 con la gestión y funcionamiento de la PKI-SAR.

5.3.5 Frecuencia y secuencia de rotación de obligaciones

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

	POLÍTICA DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN DE INFRAESTRUCTURA DE CLAVE PÚBLICA DEL SERVICIO DE ADMINISTRACIÓN DE RENTAS DE LA REPUBLICA DE HONDURAS SECRETARÍA GENERAL	Código: POL-GIF-GGI-NDP-019- V2 Fecha de vigencia: FEBRERO - 2023
---	---	---

5.3.6 Sanciones por acciones no autorizadas

Las sanciones y procedimientos a seguir para el cumplimiento de los controles del personal son definidos en el Régimen de Carrera de Empleados y Funcionarios en el Servicio de Administración de Rentas (RECAEFUSAR).

5.3.7 Requisitos de contratación de terceros

El SAR está en la potestad de realizar contrataciones de recursos externos a la entidad, a través 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 cláusulas específicas a los roles de gestión y estipula penalizaciones para las acciones no autorizadas.
- El SAR no cuenta con la disponibilidad del talento humano para ejercer los roles contratados.
- Los contratistas deben cumplir con los requisitos estipulados en el punto 5.3.1. 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.

5.3.8 Documentación provista al personal

El SAR dotará a todo su personal de la información, documentación y buenas prácticas de seguridad de la información, las cuales son indispensables para el correcto cumplimiento de sus tareas y obligaciones. La documentación debe incluir, pero no restringirse, a lo siguiente:

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

	POLÍTICA DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN DE INFRAESTRUCTURA DE CLAVE PÚBLICA DEL SERVICIO DE ADMINISTRACIÓN DE RENTAS DE LA REPUBLICA DE HONDURAS SECRETARÍA GENERAL	Código: POL-GIF-GGI-NDP-019- V2 Fecha de vigencia: FEBRERO - 2023
---	---	---

- Otros documentos necesarios.

5.4 Procedimientos de auditoría de registros

5.4.1 Tipos de eventos registrados

La PKI-SAR 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.

5.4.2 Frecuencia de procesamiento de registros

Los registros serán analizados de forma periódica, mediante las auditorías de la PKI, y también podrá ser realizada a demanda de ser necesario.

	POLÍTICA DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN DE INFRAESTRUCTURA DE CLAVE PÚBLICA DEL SERVICIO DE ADMINISTRACIÓN DE RENTAS DE LA REPUBLICA DE HONDURAS SECRETARÍA GENERAL	Código: POL-GIF-GGI-NDP-019- V2 Fecha de vigencia: FEBRERO - 2023
---	---	---

5.4.3 Período de Retención de los registros de Auditoría

La totalidad de la información generada en los registros de eventos debe ser mantenida en la base de datos de la PKI, por la totalidad del periodo de vida de la PKI.

5.4.4 Protección de los registros de auditoría

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

5.4.5 Procedimientos de respaldo de los registros de auditoría

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

5.4.6 Sistema de recolección de registros

Los eventos significativos generados por la AC y por las AR son convenientemente almacenados en los sistemas internos de la PKI-SAR.

5.4.7 Notificación al sujeto causante del evento

No se contempla.

5.4.8 Análisis de vulnerabilidades

Los eventos en el proceso de auditoría 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.

	POLÍTICA DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN DE INFRAESTRUCTURA DE CLAVE PÚBLICA DEL SERVICIO DE ADMINISTRACIÓN DE RENTAS DE LA REPUBLICA DE HONDURAS SECRETARÍA GENERAL	Código: POL-GIF-GGI-NDP-019- V2 Fecha de vigencia: FEBRERO - 2023
---	---	---

5.5 Archivado de registros

5.5.1 Tipo de eventos archivados

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

5.5.2 Período de conservación de registros

La totalidad de la información y documentación correspondiente a los certificados será resguardada durante un período no menor a 5 años.

5.5.3 Protección del archivo

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



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

SECRETARÍA GENERAL

Código:
POL-GIF-GGI-NDP-019-
V2

Fecha de vigencia:
FEBRERO - 2023

5.5.4 Procedimientos de copia de respaldo del archivo

En todo momento existirá una copia de seguridad de todos los archivos considerados críticos para la realización de la actividad de la PKI-SAR como Prestador de Servicios de Confianza.

5.5.5 Requisito para el sellado de tiempo de los registros

PKI-SAR garantiza el registro del tiempo en que se crean los archivos. El instante de tiempo de los sistemas proviene de una fuente segura que constata la fecha y hora. La fuente de tiempos utilizada será la AST.

5.5.6 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 físicos de soportes y archivos informáticos, con el fin de ser capaces de verificar la integridad, entre otros aspectos.

5.6 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 confían 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 PKI-SAR.

	POLÍTICA DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN DE INFRAESTRUCTURA DE CLAVE PÚBLICA DEL SERVICIO DE ADMINISTRACIÓN DE RENTAS DE LA REPUBLICA DE HONDURAS SECRETARÍA GENERAL	Código: POL-GIF-GGI-NDP-019- V2 Fecha de vigencia: FEBRERO - 2023
---	---	---

5.7 Recuperación por compromiso de clave o catástrofe

5.7.1 Gestión de Incidentes y Vulnerabilidades

El SAR tiene establecido un Plan de Continuidad de Negocio que define las acciones a realizar, recursos a utilizar y personal a emplear en el caso de producirse un acontecimiento intencionado o accidental que inutilice o degrade los recursos y los servicios de certificación prestados por su PKI.

El Plan de Continuidad contempla, entre otros aspectos, los siguientes:

- La redundancia de los componentes más críticos.
- La puesta en marcha de un centro de respaldo alternativo.
- El chequeo completo y periódico de los servicios de copia de respaldo.

5.7.2 Actuación ante datos y software corruptos

Esta contingencia está contemplada en el Plan de Continuidad de Negocio del SAR.

5.7.3 Procedimiento ante compromiso de clave

Esta contingencia está contemplada en el Plan de Continuidad de Negocio del SAR, así como el procedimiento a seguir, y que determina, entre otras, las siguientes acciones a tomar:

- Detener la prestación del servicio afectado.
- Revocar los certificados que pudieran verse afectados.
- Informar de los hechos a las partes afectadas.
- Estudiar la necesidad de cese de actividades de PSC según la DPC y la legislación vigente.

	POLÍTICA DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN DE INFRAESTRUCTURA DE CLAVE PÚBLICA DEL SERVICIO DE ADMINISTRACIÓN DE RENTAS DE LA REPUBLICA DE HONDURAS SECRETARÍA GENERAL	Código: POL-GIF-GGI-NDP-019- V2 Fecha de vigencia: FEBRERO - 2023
---	---	---

5.7.4 Continuidad del negocio después de un desastre

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.

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.

5.8 Cese de una Autoridad Certificadora (AC)

5.8.1 Autoridad de Certificación

En el caso de cese de actividad de la Autoridad de Certificación del Servicio de Administración de Rentas, es responsabilidad del mismo, 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.

	POLÍTICA DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN DE INFRAESTRUCTURA DE CLAVE PÚBLICA DEL SERVICIO DE ADMINISTRACIÓN DE RENTAS DE LA REPUBLICA DE HONDURAS SECRETARÍA GENERAL	Código: POL-GIF-GGI-NDP-019- V2 Fecha de vigencia: FEBRERO - 2023
---	---	---

5.8.2 Autoridad de Registro

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

6. CONTROLES DE SEGURIDAD TÉCNICA Generación e instalación del par de claves

6.1.1 Generación del par de claves

Los pares de llaves correspondientes a los componentes internos de PKI-SAR, específicamente ACR 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 a lo dispuesto en la PC correspondiente a cada certificado.

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

6.1.2 Entrega de la llave privada al suscriptor

La Autoridad de Registro será responsable de garantizar la entrega al Suscriptor habilitando los mecanismos para su descarga y posterior uso, propios de cada certificado y será establecido en la PC correspondiente a cada certificado.

	POLÍTICA DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN DE INFRAESTRUCTURA DE CLAVE PÚBLICA DEL SERVICIO DE ADMINISTRACIÓN DE RENTAS DE LA REPUBLICA DE HONDURAS SECRETARÍA GENERAL	Código: POL-GIF-GGI-NDP-019- V2 Fecha de vigencia: FEBRERO - 2023
---	---	---

6.1.3 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 PC correspondiente a cada certificado.

6.1.4 Entrega de la clave pública de la AC a los terceros que confían

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

6.1.5 Tamaño de las Claves

El tamaño de claves está estipulado de la siguiente manera:

Certificado	Tamaño de clave RSA (bits)	Periodo de validez
AC Raíz	4096	20 años
AC Subordinada	4096	10 años
TSA	2048	5 años
Suscriptores	2048	Lo establecido en la correspondiente PC

6.1.6 Parámetros de generación de la clave pública y aseguramiento de la calidad

La clave pública de la AC de PKI-SAR 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

	POLÍTICA DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN DE INFRAESTRUCTURA DE CLAVE PÚBLICA DEL SERVICIO DE ADMINISTRACIÓN DE RENTAS DE LA REPUBLICA DE HONDURAS SECRETARÍA GENERAL	Código: POL-GIF-GGI-NDP-019- V2 Fecha de vigencia: FEBRERO - 2023
---	---	---

por PKI-SAR son estipulados en la PC 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 PKI-SAR, son estipulados en la PC correspondiente a cada certificado.

6.1.7 Usos admitidos de la clave (campo KeyUsage de X.509 V3)

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

La totalidad de los certificados emitidos por PKI-SAR 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.

6.2 Protección de la clave privada y controles de ingeniería de los módulos

6.2.1 Estándares para los módulos criptográficos

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

La puesta en marcha de cada una de las AC, 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 PKI-SAR emplea módulos criptográficos de hardware y software desarrollados por terceros disponibles comercialmente.

	POLÍTICA DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN DE INFRAESTRUCTURA DE CLAVE PÚBLICA DEL SERVICIO DE ADMINISTRACIÓN DE RENTAS DE LA REPUBLICA DE HONDURAS SECRETARÍA GENERAL	Código: POL-GIF-GGI-NDP-019- V2 Fecha de vigencia: FEBRERO - 2023
---	---	---

6.2.2 Control multipersona (k de n) de la clave privada

Las claves privadas de las AC 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.

6.2.3 Resguardo de la clave privada

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

6.2.4 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.

6.2.5 Archivo de la clave privada

Referirse a los numerales 6.2.3. Resguardo de la clave privada y 6.2.4. Respaldo de la clave privada.

6.2.6 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.

6.2.7 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 PKI-SAR que utilizan dichos módulos y se almacenan cifradas.

	POLÍTICA DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN DE INFRAESTRUCTURA DE CLAVE PÚBLICA DEL SERVICIO DE ADMINISTRACIÓN DE RENTAS DE LA REPUBLICA DE HONDURAS SECRETARÍA GENERAL	Código: POL-GIF-GGI-NDP-019- V2 Fecha de vigencia: FEBRERO - 2023
---	---	---

6.2.8 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.

6.2.9 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.

6.2.10 Método de destrucción de la clave privada

En el caso de los certificados, como se establezca en la PC correspondiente a cada certificado.

6.2.11 Clasificación de los módulos criptográficos

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

6.3 Otros Aspectos de la Administración del Par de Claves

6.3.1 Archivo de la Clave Pública

Es responsabilidad de PKI-SAR mantener un archivo de todos los certificados, los cuales deben incluir las claves públicas, emitidos por un periodo mínimo de cinco (5) años. El control de dicho registro es deber de los Administradores de cada una de las AC de PKI-SAR. 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.



6.3.2 Períodos Operativos de los certificados y período para uso del par de claves

El certificado y par claves, de la ACR del SAR tiene una validez de veinte (20) años, el de la Autoridad Certificadora Subordinada del SAR una validez de dieciocho (18) años y el certificado de la AST veinte (20) años.

El período de validez del resto de certificados vendrá establecido en las PC que corresponda.

Un certificado no puede ser utilizado después del periodo de validez, aunque los terceros que confían pueden utilizarlo para verificar datos históricos teniendo en cuenta que no tendrán un servicio de verificación en línea.

6.4 Datos de activación

6.4.1 Instalación y generación de los datos de activación

Para la instalación de una AC 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.

6.4.2 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.

	POLÍTICA DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN DE INFRAESTRUCTURA DE CLAVE PÚBLICA DEL SERVICIO DE ADMINISTRACIÓN DE RENTAS DE LA REPUBLICA DE HONDURAS SECRETARÍA GENERAL	Código: POL-GIF-GGI-NDP-019- V2 Fecha de vigencia: FEBRERO - 2023
---	---	---

6.4.3 Otros Aspectos referentes a los datos de activación

No estipulado.

6.5 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 auditorías externas o internas e inspecciones.

6.5.1 Requerimientos técnicos específicos de seguridad informática

Los datos concernientes a este apartado se consideran información confidencial y solo se proporcionan a quien acredite la necesidad de conocerlos.

6.5.2 Evaluación del nivel de seguridad informática

La PKI-SAR evalúa de forma permanente su nivel de seguridad de cara a identificar posibles debilidades y establecer las correspondientes acciones correctoras mediante auditorías externas e internas, así con la realización continua de controles de seguridad.

6.6 Controles de seguridad del 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.

6.6.1 Controles de desarrollo de sistema

Los requisitos de seguridad son exigibles, desde su inicio, tanto en la adquisición como en el desarrollo e implementación de los sistemas informáticos. El proceso de evolución de los sistemas informáticos identifica la necesidad de realizar correcciones de emergencias o nuevas versiones de software, evaluar su impacto y documentación.



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

SECRETARÍA GENERAL

Código:
POL-GIF-GGI-NDP-019-
V2

Fecha de vigencia:
FEBRERO - 2023

6.6.2 Controles de administración de seguridad

La integridad de la información y los sistemas de la PKI-SAR, es protegida contra virus, software malicioso y no autorizado. La PKI-SAR lleva a cabo el levantamiento y mantenimiento de un inventario de activos tecnológicos, y realiza una clasificación coherente de acuerdo con sus necesidades de protección.

6.6.3 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 PKI-SAR.

6.7 Controles de seguridad de redes

La PKI-SAR segmenta sus sistemas en redes o zonas, teniendo en cuenta la relación funcional, lógica y física entre los sistemas y servicios confiables.

El acceso a Internet a los Centros de Datos está redundado y, adicionalmente, el servicio es proporcionado por operadores diferentes. Los mecanismos de conmutación de operadores son automáticos.

Los medios de comunicación mediante redes públicas, que la PKI-SAR utiliza en el desarrollo de sus actividades, utilizan suficientes mecanismos de seguridad, para evitar o controlar adecuadamente cualquier agresión externa a través de estas redes.

6.8 Sellado de tiempo

El formato de los Sellos de Tiempo emitidos por la Autoridad de Sellado de Tiempo es según lo indicado en la RFC 3161 – “Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP)” y la normativa ETSI 102 023 – “Requisitos para las Políticas de las Autoridades de Sellado de Tiempo”.

	POLÍTICA DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN DE INFRAESTRUCTURA DE CLAVE PÚBLICA DEL SERVICIO DE ADMINISTRACIÓN DE RENTAS DE LA REPUBLICA DE HONDURAS SECRETARÍA GENERAL	Código: POL-GIF-GGI-NDP-019- V2 Fecha de vigencia: FEBRERO - 2023
---	---	---

6.9 Otros controles adicionales

6.9.1 Control de la capacidad de prestación de los servicios

La PKI-SAR realiza controles periódicos del grado de demanda de los servicios relacionados con su actividad como Prestador de Servicios de Confianza y de la capacidad de su infraestructura para proveer dichos servicios, como por ejemplo el sistema de información de consumos, grado de disponibilidad y ocupación de los recursos. Estos controles permiten identificar futuras inversiones en infraestructura para mantener la capacidad de prestación de los servicios.

6.9.2 Control de desarrollo de sistemas y aplicaciones informáticas

Antes de abordar cualquier nuevo proyecto de desarrollo de software, o en caso de requerirse un cambio en algún desarrollo existente, se valorará el establecimiento de controles adicionales a los especificados en los procedimientos en vigor.

7. PERFILES DE CERTIFICADOS OCSP Y CRLS

7.1 Perfil de certificado

7.1.1 Número de versión

PKI-SAR es compatible con certificados X.509 versión 3 (X.509 V3).

7.1.2 Extensiones del Certificado

Las extensiones utilizadas de forma genérica en los certificados son:

- KeyUsage. Calificada como crítica.
- BasicConstraints. Calificada como crítica.
- CertificatePolicies. Calificada como no crítica.
- SubjectAlternativeName. Calificada como no crítica.
- CRLDistributionPoint. Calificada como no crítica.

	POLÍTICA DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN DE INFRAESTRUCTURA DE CLAVE PÚBLICA DEL SERVICIO DE ADMINISTRACIÓN DE RENTAS DE LA REPUBLICA DE HONDURAS SECRETARÍA GENERAL	Código: POL-GIF-GGI-NDP-019-V2 Fecha de vigencia: FEBRERO - 2023
---	---	--

Las Políticas de Certificación de PKI-SAR pueden establecer variaciones en conjunto de las extensiones utilizadas por cada tipo de certificado.

A continuación, se detalla el contenido de las extensiones más significativas de la AC R del SAR:

Extensión del certificado Autoridad Certificadora Raíz del SAR				
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
Subject Key Identifier	-	<Resumen SHA-1 (160 bits) de la llave pública del campo Subject Public Key Info del emisor>	Si	No
Key Usage	-	Certificate Signing, Off-line CRL Signing, CRL Signing (06)	Si	Si
Extended Key Usage	-	-	Si	No
Certificate Policies	policyIdentifier (OID)	1.3.6.1.4.1.52089.2.1	Si	No
	cPSuri	URL: https://www.sar.gob.hn/firma electronica/		
Basic Constraints	Subject Type	CA	Si	Si
	Path Length Constraint	None	-	-

A continuación, se detalla el contenido de las extensiones más significativas de la Autoridad Subordinada del SAR:

	POLÍTICA DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN DE INFRAESTRUCTURA DE CLAVE PÚBLICA DEL SERVICIO DE ADMINISTRACIÓN DE RENTAS DE LA REPUBLICA DE HONDURAS SECRETARÍA GENERAL	Código: POL-GIF-GGI-NDP-019- V2 Fecha de vigencia: FEBRERO - 2023
---	---	---

Extensión del certificado Autoridad Subordinada del SAR				
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
Subject Key Identifier	-	Resumen SHA-1 (160 bits) de la llave pública del campo Subject Public Key Info del emisor	Si	No
Key Usage	-	Certificate Signing, Off-line CRL Signing	Si	Si
Extended Key Usage	-	-	Si	No
Certificate Policies	policyIdentifier (OID)	1.3.6.1.4.1.52089.2.1	Si	No
	cPSuri	URL: https://www.sar.gob.hn/firmaelectronica/		
Basic Constraints	Subject Type	CA	Si	Si
	Path Length Constraint	None	-	-
CRL Distribution Points	Distribution Point Name (URI)	http://pki.sar.gob.hn/crlsar/arl.crl	Si	No
Authority Information Access	CAIssuers (URI)	http://pki.sar.gob.hn/crlsar/caoot.crt	Si	

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.

	POLÍTICA DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN DE INFRAESTRUCTURA DE CLAVE PÚBLICA DEL SERVICIO DE ADMINISTRACIÓN DE RENTAS DE LA REPUBLICA DE HONDURAS SECRETARÍA GENERAL	Código: POL-GIF-GGI-NDP-019- V2 Fecha de vigencia: FEBRERO - 2023
---	---	---

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 objetos (OID) de la PC expedidos por la PKI-SAR, se describe en la PC correspondiente.

7.1.7 Uso de la extensión “PolicyConstraints”

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

7.1.8 Sintaxis y semántica de los “PolicyQualifier”

La extensión “Certificate Policies” contiene los siguientes “Policy Qualifiers”:

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

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

	POLÍTICA DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN DE INFRAESTRUCTURA DE CLAVE PÚBLICA DEL SERVICIO DE ADMINISTRACIÓN DE RENTAS DE LA REPUBLICA DE HONDURAS SECRETARÍA GENERAL	Código: POL-GIF-GGI-NDP-019- V2 Fecha de vigencia: FEBRERO - 2023
---	---	---

7.1.9 Tratamiento semántico para la extensión crítica “CertificatePolicies”

La extensión “Certificate Policy” incluye el campo OID de política, que identifica la política asociada al certificado por parte de la PKI-SAR, así como los dos campos relacionados en el apartado anterior.

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 las 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



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

SECRETARÍA GENERAL

Código:
POL-GIF-GGI-NDP-019-
V2

Fecha de vigencia:
FEBRERO - 2023

7.3 Perfil de OCSP

7.3.1 Número de versión

La AV admite peticiones firmadas y las extensiones definidas en RFC 2560.

7.3.2 Extensiones OCSP

Las respuestas OCSP del servicio de información y consulta sobre el estado de validez de los certificados incluyen, para las peticiones que lo soliciten, la extensión global “nonce”, que se utiliza para vincular una petición con una respuesta, de forma que se puedan prevenir ataques de repetición.

8. AUDITORÍAS DE CUMPLIMIENTO Y OTROS CONTROLES

8.1 Frecuencia o circunstancias de los controles para cada Autoridad

Se llevará a cabo una auditoría externa sobre PKI-SAR de forma regular una vez al año. Con ello se garantiza la adecuación de su funcionamiento y operativa con las estipulaciones incluidas en esta DPC y las PC correspondientes.

8.2 Identificación/cualificación del auditor

El auditor que verifique y compruebe la correcta operatividad del Prestador de Servicios de Confianza de la PKI-SAR, debe ser una persona o profesional con la suficiente titulación oficial y la adecuada experiencia sobre la materia a auditar de acuerdo con la legislación que se encuentre en vigor en ese momento. Al menos, debe acreditar los siguientes requisitos:

- Adecuada capacitación y experiencia en PKI, seguridad, tecnologías criptográficas y procesos de auditoría.
- Independencia a nivel organizativo de la Autoridad de la PKI-SAR.

	POLÍTICA DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN DE INFRAESTRUCTURA DE CLAVE PÚBLICA DEL SERVICIO DE ADMINISTRACIÓN DE RENTAS DE LA REPUBLICA DE HONDURAS SECRETARÍA GENERAL	Código: POL-GIF-GGI-NDP-019- V2 Fecha de vigencia: FEBRERO - 2023
---	---	---

Junto con el informe obtenido de la auditoría, figurará la identificación de los auditores. El informe resultado de la auditoría será firmado por los auditores y por el responsable del ente auditado.

8.3 Relación entre el auditor y la autoridad auditada

Al margen de la función de auditoría, el auditor externo y la parte auditada (PKI-SAR) no deben tener relación alguna que pueda derivar en un conflicto de intereses.

En los casos en los que las auditorías se elaboran por personal externo a la PKI-SAR, se establecen las medidas y controles necesarios para regular los requisitos de auditoría, el alcance, acceso a información sensible y demás acuerdos de confidencialidad y responsabilidad sobre los activos.

8.4 Aspectos cubiertos por los controles

Se realizarán los siguientes controles:

- 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.

8.5 Toma de decisiones frente a la detección de deficiencias

La identificación de deficiencias detectadas como resultado de la auditoría dará lugar a la adopción de medidas correctivas. El Comité de Firma Electrónica, en colaboración con el auditor, serán los responsables de la determinación de estas.

En el caso de observarse deficiencias graves, el Comité de Firma Electrónica adoptará, entre otras, las siguientes decisiones: suspensión temporal de las operaciones hasta que las deficiencias se corrijan, revocación del certificado de la

	POLÍTICA DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN DE INFRAESTRUCTURA DE CLAVE PÚBLICA DEL SERVICIO DE ADMINISTRACIÓN DE RENTAS DE LA REPUBLICA DE HONDURAS SECRETARÍA GENERAL	Código: POL-GIF-GGI-NDP-019- V2 Fecha de vigencia: FEBRERO - 2023
---	---	---

Autoridad Certificadora, cambios en el personal implicado y auditorías globales más frecuentes.

De igual manera la PKI-SAR actuará diligentemente para subsanar el error o defecto detectado en el menor espacio de tiempo posible.

8.6 Comunicación de resultados

El equipo auditor comunicará los resultados de la auditoría al Comité de Firma Electrónica, al Gestor de Seguridad de PKI-SAR, así como a los administradores de PKI-SAR y del área en la que se detecten incidencias.

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 son estipuladas en la PC que corresponda.

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 los servicios de información del estado de los certificados a través de CRL o del OCSP de forma gratuita.

	POLÍTICA DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN DE INFRAESTRUCTURA DE CLAVE PÚBLICA DEL SERVICIO DE ADMINISTRACIÓN DE RENTAS DE LA REPUBLICA DE HONDURAS SECRETARÍA GENERAL	Código: POL-GIF-GGI-NDP-019- V2 Fecha de vigencia: FEBRERO - 2023
---	---	---

9.1.4 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 en su respectiva PC.

9.1.5 Política de reembolso

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

9.2 Responsabilidades económicas

9.2.1 Seguro de Responsabilidad civil

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

9.2.2 Otros activos

No estipulado.

9.2.3 Seguros y garantías para entidades finales

No estipulado.

9.3 Confidencialidad de la información

Toda la información que, en conocimiento del SAR como Prestador de Servicios de Certificación en relación con los datos personales de sus usuarios, debe ser

	POLÍTICA DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN DE INFRAESTRUCTURA DE CLAVE PÚBLICA DEL SERVICIO DE ADMINISTRACIÓN DE RENTAS DE LA REPUBLICA DE HONDURAS SECRETARÍA GENERAL	Código: POL-GIF-GGI-NDP-019- V2 Fecha de vigencia: FEBRERO - 2023
---	---	---

mantenida en estricta confidencialidad. Así mismo, todos sus funcionarios(as) y/o empleados(as), proveedores, y contratistas deben mantener estricta confidencialidad de toda la información que adquieran o manejen, en relación con todos los elementos vinculados a la PKI-SAR.

9.3.1 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 PKI-SAR.
- La información sobre operaciones que lleve a cabo PKI-SAR.
- La información referente a los parámetros de seguridad, control y procedimientos de auditoría.

9.3.2 Información no confidencial

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

- La presente Declaración de Prácticas de Certificación.
- Políticas de Certificación.
- La lista de los certificados suspendidos o revocados.

9.3.3 Responsabilidad de proteger la información confidencial.

El recurso humano del Servicio de Administración de Rentas y otros organismos externos a ellos que participen en tareas relacionadas a la operación de PKI-SAR, están obligados al deber de secreto profesional, y por lo tanto, sujetos a la normativa aplicable del Régimen de Carrera de Empleados y Funcionarios en el Servicio de Administración de Rentas (RECAEFUSAR).

	POLÍTICA DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN DE INFRAESTRUCTURA DE CLAVE PÚBLICA DEL SERVICIO DE ADMINISTRACIÓN DE RENTAS DE LA REPUBLICA DE HONDURAS SECRETARÍA GENERAL	Código: POL-GIF-GGI-NDP-019- V2 Fecha de vigencia: FEBRERO - 2023
---	---	---

9.4 Protección de la información personal

La PKI-SAR 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, que garantiza el derecho al honor, la intimidad y a la imagen de toda persona.

9.5 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.

9.6 Obligaciones y garantías

9.6.1 Obligaciones de las AC

Las PKI-SAR deben acogerse a las obligaciones dispuestas en este numeral, la cual tienen las siguientes obligaciones:

- Realizar sus operaciones en cumplimiento de esta DPC.
- Resguardar sus claves privadas.
- Emitir certificados según lo estipulado en las PC correspondientes.
- Emitir certificados de acuerdo con el estándar X.509 V3.
- 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



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

SECRETARÍA GENERAL

Código:
POL-GIF-GGI-NDP-019-
V2

Fecha de vigencia:
FEBRERO - 2023

6.8.9 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 4.9.7 Frecuencia de emisión de CRL.

- Publicar esta DPC y las PC correspondientes en el sitio web referido en el apartado 2.1 Repositorio.
- Emitir comunicados sobre los cambios de esta DPC y de las PC según lo estipula el apartado 9.6.11 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 PC 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 de Certificado electrónico, delimitando su utilización solo a las tareas del servicio de certificación, salvo orden judicial o solicitud del Suscriptor o Suscriptor mismo.

9.6.2 Obligaciones de la AR

Las AR operativas en PKI-SAR 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.

	POLÍTICA DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN DE INFRAESTRUCTURA DE CLAVE PÚBLICA DEL SERVICIO DE ADMINISTRACIÓN DE RENTAS DE LA REPUBLICA DE HONDURAS SECRETARÍA GENERAL	Código: POL-GIF-GGI-NDP-019- V2 Fecha de vigencia: FEBRERO - 2023
---	---	---

- 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.

9.6.3 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 PKI-SAR 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 PC 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.

	POLÍTICA DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN DE INFRAESTRUCTURA DE CLAVE PÚBLICA DEL SERVICIO DE ADMINISTRACIÓN DE RENTAS DE LA REPUBLICA DE HONDURAS SECRETARÍA GENERAL	Código: POL-GIF-GGI-NDP-019- V2 Fecha de vigencia: FEBRERO - 2023
---	---	---

- 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 PC.

9.6.4 Obligaciones de los terceros que confían o acepten los certificados

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

- Limitar el empleo de los certificados a los usos permitidos de los mismos, según lo dispuesto en las extensiones de los certificados y la PC 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 confía.
- 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 PKI-SAR sobre cualquier situación anómala relacionada al certificado y que pueda resultar en la revocación de este.

9.7 Exención de responsabilidades

La PKI-SAR 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 PC específicas.

La PKI-SAR sólo responderá por los daños y perjuicios que en el ejercicio de su actividad ocasionen por la certificación u homologación de certificados de firmas

	POLÍTICA DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN DE INFRAESTRUCTURA DE CLAVE PÚBLICA DEL SERVICIO DE ADMINISTRACIÓN DE RENTAS DE LA REPUBLICA DE HONDURAS SECRETARÍA GENERAL	Código: POL-GIF-GGI-NDP-019- V2 Fecha de vigencia: FEBRERO - 2023
---	---	---

electrónicas. En todo caso corresponde a PKI-SAR demostrar que actuó con la debida diligencia.

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

9.8 Limitaciones de las responsabilidades

La PKI-SAR no será responsable 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 PKI-SAR 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 PKI-SAR 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 período de validez del certificado electrónico o el Prestador de Servicios de Certificación le notifique la extinción de su vigencia.
- 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 PKI-SAR.



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

SECRETARÍA GENERAL

Código:
POL-GIF-GGI-NDP-019-
V2

Fecha de vigencia:
FEBRERO - 2023

La PKI-SAR tampoco será responsable 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, entre otros, 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.
- Cuando no tenga en cuenta la revocación o pérdida de vigencia del certificado electrónico publicada en el sitio web de PKI-SAR o cuando no verifique la Firma Electrónica.

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

9.9 Indemnizaciones

No estipulado.

9.9.1 Indemnizaciones de la AC

No estipulado.

9.9.2 Indemnizaciones de los suscriptores

No estipulado.

9.9.3 Indemnizaciones de las partes que confían

No estipulado.

	POLÍTICA DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN DE INFRAESTRUCTURA DE CLAVE PÚBLICA DEL SERVICIO DE ADMINISTRACIÓN DE RENTAS DE LA REPUBLICA DE HONDURAS SECRETARÍA GENERAL	Código: POL-GIF-GGI-NDP-019- V2 Fecha de vigencia: FEBRERO - 2023
---	---	---

9.10 Período de validez de este documento

9.10.1 Periodo

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

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

9.10.2 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 debe ser eliminada de los repositorios de PKI-SAR, si bien se conservará en archivo durante cinco (5) años.

9.10.3 Efectos de la terminación

Las obligaciones y restricciones detalladas en esta DPC, estipuladas con respecto a: auditorías, información confidencial, obligaciones y responsabilidades de la PKI-SAR, nacidas bajo su vigencia, subsistirán tras su renovación o derogación por una nueva versión.

9.11 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 por escrito o mediante correo electrónico que tenga como remitente a cualquiera de las direcciones contenidas en el punto 6.4 Administración de las Políticas. Las comunicaciones

	POLÍTICA DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN DE INFRAESTRUCTURA DE CLAVE PÚBLICA DEL SERVICIO DE ADMINISTRACIÓN DE RENTAS DE LA REPUBLICA DE HONDURAS SECRETARÍA GENERAL	Código: POL-GIF-GGI-NDP-019- V2 Fecha de vigencia: FEBRERO - 2023
---	---	---

electrónicas producirán sus efectos una vez que las reciba el destinatario al que van dirigidas.

9.12 Modificaciones de este documento

9.12.1 Procedimiento para las Modificaciones

El Comité de Firma Electrónica del SAR es la única entidad con la potestad para realizar y aprobar cambios sobre la DPC y las PC de la PKI-SAR.

9.12.2 Periodo y mecanismo de notificación

El Comité de Firma Electrónica del SAR revisará anualmente la DPC y las PC y cada vez que deba llevarse a cabo alguna modificación de estas.

Cualquier modificación en la presente DPC y PC correspondiente será publicada de forma inmediata en la URL de acceso a la misma.

9.12.3 Circunstancias bajo las cuales debe cambiarse un OID

Las modificaciones significativas de las condiciones de los servicios y responsabilidades o limitaciones de uso de los certificados, pueden ocasionar un cambio de política del servicio y su identificación (OID), así como el alcance a la nueva DPC o PC.

9.13 Resolución de conflictos

Todas las reclamaciones entre usuarios y la PKI-SAR deben ser notificadas por la parte en disputa, a la AAC y al Comité de Firma Electrónica con el fin de expeditar la resolución que corresponda.

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 vía administrativa al Tribunal Contencioso Administrativo correspondiente.

	POLÍTICA DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN DE INFRAESTRUCTURA DE CLAVE PÚBLICA DEL SERVICIO DE ADMINISTRACIÓN DE RENTAS DE LA REPUBLICA DE HONDURAS SECRETARÍA GENERAL	Código: POL-GIF-GGI-NDP-019- V2 Fecha de vigencia: FEBRERO - 2023
---	---	---

9.14 Normativa aplicable

La totalidad de las normativas aplicables a las operaciones y funcionamiento de PKI-SAR, 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 el Diario Oficial La Gaceta del 11 de diciembre del 2013 y sus reformas, su Reglamento y demás legislación aplicable.

9.15 Cumplimiento de la legislación aplicable

Es obligación de la AAC asegurar el cumplimiento de la legislación aplicable recogida en el numeral anterior.

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 esta DPC y de las PC correspondientes.

9.16.2 Resolución de conflictos en la vía judicial

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

9.17 Otras Estipulaciones

No se consideran otras estipulaciones.