

ADMINISTRACIÓN FEDERAL DE INGRESOS PÚBLICOS

AUTORIDAD CERTIFICANTE

MANUAL DE PROCEDIMIENTOS PARA CERTIFICADOS DIGITALES

OID: 2.16.32.1.1.1

DOCUMENTO RESERVADO, SUJETO A NORMAS DE
CONFIDENCIALIDAD. PROHIBIDA SU DIFUSIÓN DESDE EL PUNTO 4.5
INCLUSIVE
Y HASTA EL FINAL DEL PRESENTE DOCUMENTO

Versión 1 – 19/12/08

ÍNDICE

1. - INTRODUCCIÓN.....	5
1.1– DESCRIPCIÓN GENERAL.....	5
1.2. - IDENTIFICACIÓN.....	5
1.3. - PARTICIPANTES Y APLICABILIDAD.....	5
1.3.1. – <i>Certificador</i>	5
1.3.2. - <i>Autoridad de Registro (AR)</i>	5
1.3.3. - <i>Suscriptores de certificados</i>	6
1.3.4. - <i>Aplicabilidad</i>	7
1.4. - CONTACTOS.....	7
2. - ASPECTOS GENERALES DEL MANUAL DE PROCEDIMIENTOS.....	7
2.1. – OBLIGACIONES.....	7
2.1.1. - <i>Obligaciones del certificador</i>	7
2.1.2. - <i>Obligaciones de la Autoridad de Registro</i>	7
2.1.3. – <i>Obligaciones de los suscriptores de los certificados</i>	8
2.1.4. - <i>Obligaciones de los terceros usuarios</i>	8
2.1.5. - <i>Obligaciones del servicio de repositorio</i>	8
2.2. – RESPONSABILIDADES.....	8
2.3. – RESPONSABILIDAD FINANCIERA.....	8
2.3.1 <i>Responsabilidad Financiera del Certificador</i>	8
2.4. - INTERPRETACIÓN Y APLICACIÓN DE LAS NORMAS.....	8
2.4.1. - <i>Legislación aplicable</i>	8
2.4.2. - <i>Forma de interpretación y aplicación</i>	9
2.4.3. - <i>Procedimientos de resolución de conflictos</i>	9
2.5. – ARANCELES.....	9
2.6. - PUBLICACIÓN Y REPOSITORIOS DE CERTIFICADOS Y LISTAS DE CERTIFICADOS REVOCADOS (CRLs).....	10
2.6.1. - <i>Publicación de información del certificador</i>	10
2.6.2. - <i>Frecuencia de publicación</i>	10
2.6.3. - <i>Controles de acceso a la información</i>	10
2.6.4. – <i>Repositorios de certificados y listas de revocación</i>	11
2.7. – AUDITORIAS.....	12
2.8. – CONFIDENCIALIDAD.....	12
2.8.1. - <i>Información confidencial</i>	12
2.8.2. - <i>Información no confidencial</i>	12
2.8.3. – <i>Publicación de información sobre la revocación o suspensión de un certificado</i>	13
2.8.4. – <i>Divulgación de información a autoridades judiciales</i>	13
2.8.5. – <i>Divulgación de información como parte de un proceso judicial o administrativo</i>	13
2.8.6. - <i>Divulgación de información por solicitud del suscriptor</i>	13
2.8.7. – <i>Otras circunstancias de divulgación de información</i>	14
2.9. - DERECHOS DE PROPIEDAD INTELECTUAL.....	14
3- IDENTIFICACIÓN Y AUTENTICACIÓN.....	15
3.1. - REGISTRO INICIAL.....	15
3.1.1. - <i>Tipos de Nombres</i>	15
3.1.2.- <i>Necesidad de Nombres Distintivos</i>	16
3.1.3.- <i>Reglas para la interpretación de nombres</i>	16
3.1.4. - <i>Unicidad de nombres</i>	17
3.1.5.- <i>Procedimiento de resolución de disputas sobre nombres</i>	17
3.1.6.- <i>Reconocimiento, autenticación y rol de las marcas registradas</i>	17
3.1.7. - <i>Métodos para comprobar la posesión de la clave privada</i>	17
3.1.8.- <i>Autenticación de la identidad de personas jurídicas públicas o privadas</i>	18
3.1.9. - <i>Autenticación de la identidad de personas físicas</i>	18
3.2.- <i>GENERACIÓN DE NUEVO PAR DE CLAVES (RUTINA DE “RE KEY”)</i>	21

3.3.- GENERACIÓN DE NUEVO PAR DE CLAVES DESPUÉS DE UNA REVOCACIÓN – SIN COMPROMISO DE CLAVE.....	22
3.4. - REQUERIMIENTO DE REVOCACIÓN	22
3.4.1 Revocación a solicitud del titular del certificado digital.....	22
3.4.2 Revocación por parte de la AFIP.....	24
4. - CICLO DEL CERTIFICADO: REQUERIMIENTOS OPERATIVOS.....	25
4.1. - SOLICITUD DE CERTIFICADO.....	25
4.1.1.- REQUISITOS PARA LA SOLICITUD DE CERTIFICADOS DIGITALES.....	26
4.1.2.- PRESENTACIÓN DE LA SOLICITUD.....	27
4.1.3.- APROBACIÓN DE LA SOLICITUD.....	30
4.1.4.- GENERACIÓN DEL PAR DE CLAVES CRIPTOGRÁFICAS DEL SUSCRIPTOR.....	30
4.1.5.- SOLICITUD DE RENOVACIÓN DEL CERTIFICADO.....	31
4.2. - EMISIÓN DEL CERTIFICADO.....	32
4.2.1.- Proceso de emisión de certificado digital de Clase 3.....	32
4.2.2.- Proceso de emisión de certificado digital de Clase 4.....	33
4.3. - ACEPTACIÓN DEL CERTIFICADO.....	34
4.3.1.- Aceptación de certificado digital de Clase 3.....	34
4.3.2.- Aceptación de certificado digital de Clase 4	35
4.4. - SUSPENSIÓN Y REVOCACIÓN DE CERTIFICADOS.....	36
4.4.1. - Causas de revocación.....	36
4.4.2. - Autorizados a solicitar la revocación.....	36
4.4.3.- Procedimientos para la solicitud de revocación	36
4.4.4. - Plazo para la solicitud de revocación.....	36
4.4.5. – Causas de suspensión.....	36
4.4.6. – Autorizados a solicitar la suspensión.....	37
4.4.7. – Procedimientos para la solicitud de suspensión.....	37
4.4.8. – Límites del período de suspensión del certificado.....	37
4.4.9. - Frecuencia de emisión de listas de certificados revocados.....	37
4.4.10. - Requisitos para la verificación de la lista de certificados revocados.....	37
4.4.11. - Disponibilidad del servicio de consulta sobre revocación y de estado del certificado.....	37
4.4.12. - Requisitos para la verificación en línea del estado de revocación.....	38
4.4.13. - Otras formas disponibles para la divulgación de la revocación.....	38
4.4.14. - Requisitos para la verificación de otras formas de divulgación de revocación.....	38
4.4.15. - Requisitos específicos para casos de compromiso de claves.....	38
4.5. - PROCEDIMIENTOS DE AUDITORÍA DE SEGURIDAD.....	38
4.5.1.- Generación y mantenimiento de archivos de auditoría.....	39
4.5.2.- Copias de resguardo de archivos de transacciones de auditoría.....	41
4.6. - ARCHIVO DE REGISTROS DE EVENTOS.....	42
4.7. – CAMBIO DE CLAVES CRIPTOGRÁFICAS DE LA AC DE LA AFIP.....	42
4.8. - PLAN DE CONTINGENCIA Y RECUPERACIÓN ANTE DESASTRES.....	43
4.9. – PLAN DE CESE DE ACTIVIDADES.....	43
5. - CONTROLES DE SEGURIDAD FÍSICA, FUNCIONALES Y PERSONALES.....	43
5.1.- CONTROLES DE SEGURIDAD FÍSICA.....	43
5.2. - CONTROLES FUNCIONALES.....	47
5.2.1.- Roles.....	47
5.2.2.- Correspondencia roles – llaves del HSM.....	50
5.2.3.- Roles – Altas y modificaciones de roles.....	51
5.2.4.- Roles - Cese de funciones – Reemplazo.....	51
5.3. - CONTROLES DE SEGURIDAD DEL PERSONAL.....	51
6. - CONTROLES DE SEGURIDAD TÉCNICA.....	53
6.1. - GENERACIÓN E INSTALACIÓN DE CLAVES.....	53
6.1.1. - Generación del par de claves criptográficas.....	53
6.1.2. - Entrega de la clave privada al suscriptor.....	54
6.1.3. - Entrega de la clave pública al emisor del certificado.....	54
6.1.4. - Disponibilidad de la clave pública del certificador.....	55
6.1.5. - Tamaño de claves.....	55

6.1.6. - <i>Generación de parámetros de claves asimétricas</i>	55
6.1.7. - <i>Verificación de calidad de los parámetros</i>	56
6.1.8. - <i>Generación de claves por hardware o software</i>	56
6.1.9.- <i>Propósitos de utilización de claves (campo “Key Usage” en certificados X.509 v.3)</i>	57
6.2. - PROTECCIÓN DE LA CLAVE PRIVADA	57
6.2.1. - <i>Estándares para dispositivos criptográficos</i>	57
6.2.2. - <i>Control “M de N” de clave privada</i>	57
6.2.3. - <i>Recuperación de clave privada</i>	58
6.2.4. - <i>Copia de seguridad de clave privada</i>	59
6.2.5. - <i>Archivo de clave privada</i>	60
6.2.6. - <i>Incorporación de claves privadas en dispositivos criptográficos</i>	60
6.2.7. - <i>Método de activación de claves privadas</i>	61
6.2.8. - <i>Método de desactivación de claves privadas</i>	61
6.2.9. - <i>Método de destrucción de claves privadas</i>	62
6.3. - OTROS ASPECTOS DE ADMINISTRACIÓN DE CLAVES	63
6.3.1.- <i>Archivo permanente de la clave pública</i>	63
6.3.2. - <i>Período de uso de clave pública y privada</i>	63
6.4. - DATOS DE ACTIVACIÓN	63
6.4.1.- <i>Generación e instalación de datos de activación</i>	63
6.4.2. - <i>Protección de los datos de activación</i>	64
6.4.3. - <i>Otros aspectos referidos a los datos de activación</i>	65
6.5. - CONTROLES DE SEGURIDAD INFORMÁTICA	65
6.5.1.- <i>Requisitos Técnicos específicos</i>	65
6.5.2.- <i>Calificaciones de seguridad computacional</i>	66
6.6. - CONTROLES TÉCNICOS DEL CICLO DE VIDA DE LOS SISTEMAS	67
6.6.1. - <i>Controles de desarrollo de sistemas</i>	67
6.6.2. - <i>Administración de controles y seguridad</i>	67
6.6.3. - <i>Calificaciones de seguridad del ciclo de vida del software</i>	67
6.7. - CONTROLES DE SEGURIDAD DE RED	67
6.8. - CONTROLES DE INGENIERÍA DE DISPOSITIVOS CRIPTOGRÁFICOS	68
7. - PERFILES DE CERTIFICADOS Y DE LISTAS DE CERTIFICADOS REVOCADOS	68
7.1. - PERFIL DEL CERTIFICADO	68
7.2. - PERFIL DE LA LISTA DE CERTIFICADOS REVOCADOS	68
7.3. - PERFIL DEL CERTIFICADO OCSP	68
8. - ADMINISTRACIÓN DE ESPECIFICACIONES	68
8.1. - PROCEDIMIENTOS DE CAMBIO DE ESPECIFICACIONES	68
8.2. - PROCEDIMIENTOS DE PUBLICACIÓN Y NOTIFICACIÓN	69
8.3. - PROCEDIMIENTOS DE APROBACIÓN	69

1. - INTRODUCCIÓN

1.1- Descripción general

El presente manual establece los procedimientos relacionados con la emisión y administración de los certificados digitales de la Autoridad Certificante de la Administración Federal de Ingresos Públicos de la República Argentina (en adelante “AC de la AFIP”). Dichos procedimientos requieren para su ejecución las funciones instrumentadas por el Sistema Informático de AC de la AFIP, desarrollado por la Subdirección General de Sistemas y Telecomunicaciones de la AFIP.

1.2. - Identificación

Nombre: Manual de Procedimientos para Certificados Digitales de la AC de la AFIP

Versión: 1

Fecha: 19/12/2008

Sitio Web: “acn.afip.gov.ar”

OID: 2.16.32.1.1.1

Lugar: Buenos Aires, Argentina

1.3. - Participantes y aplicabilidad

1.3.1. – Certificador

Los procedimientos descritos en el presente manual en sus partes pertinentes, son de aplicación obligatoria para la AFIP.

1.3.2. - Autoridad de Registro (AR)

Los procedimientos descriptos en el presente manual en sus partes pertinentes, son de aplicación obligatoria para la Autoridad de Registro y sus Puestos de Atención.

En los Puestos de Atención de la Autoridad de Registro se realizan las funciones de verificación de identidad de los solicitantes de certificados digitales y la gestión de trámites asociados.

El Sistema Informático de AC de la AFIP instrumenta un módulo que se corresponde con las funciones de los Puestos de Atención de la AR y es operado por el Responsable de AR, los Responsables de los Puestos de Atención y por los Oficiales de Registro designados.

En los documentos anexos al presente manual, bajo el título “Procedimientos de los Puestos de Atención de la Autoridad de Registro de la AFIP”, figuran los procedimientos para la designación de un Puesto de Atención, de su Responsable y de sus Oficiales de Registro, así como también sus responsabilidades y cumplimiento de funciones en relación con el proceso de gestión de certificados digitales.

1.3.3. - Suscriptores de certificados

Los procedimientos descriptos en el presente manual, en sus partes pertinentes a cada clase de certificado, son de aplicación obligatoria para los solicitantes y suscriptores de certificados.

Los solicitantes de los certificados digitales deberán ser personas físicas y poseer Clave Fiscal de nivel 3 o 4 emitida por la AFIP.

Existen tres clases de certificados digitales contemplados bajo el presente manual:

- Clase 3: Implementado por software.
- Clase 4: Implementado por hardware, por medio de un dispositivo criptográfico.

- OCSP: El suscriptor es la AFIP, usado en relación con el servicio de verificación en línea del estado de un certificado.

La clase de certificado determina su posibilidad de utilización por parte de los sistemas que implementen el esquema de firma digital.

1.3.4. - Aplicabilidad

Los procedimientos descriptos en el presente manual como en sus documentos anexos, son de aplicación obligatoria para la emisión, renovación y/o revocación de certificados digitales como así también para el proceso de certificación de la AC de la AFIP.

1.4. - Contactos

Este manual es administrado por la AFIP. Por consultas o sugerencias, por favor dirigirse a:

Por nota: Responsable de la AC de la AFIP
 Mesa de Entradas Paseo Colón 635 - CABA

Por e-mail: acn@afip.gov.ar

Personalmente: ante un Puesto de Atención de la AR habilitado.

Mesa de Ayuda: 0-810-999-2347

Domicilio constituido a los efectos legales: Paseo Colón 635 – CABA

2. - ASPECTOS GENERALES DEL MANUAL DE PROCEDIMIENTOS

2.1. – Obligaciones

2.1.1. - Obligaciones del certificador

No hay procedimientos aplicables a este punto.

2.1.2. - Obligaciones de la Autoridad de Registro

No hay procedimientos aplicables a este punto.

2.1.3. – Obligaciones de los suscriptores de los certificados

No hay procedimientos aplicables a este punto.

2.1.4. - Obligaciones de los terceros usuarios

No hay procedimientos aplicables a este punto.

2.1.5. - Obligaciones del servicio de repositorio

No hay procedimientos aplicables a este punto.

2.2. – Responsabilidades

No hay procedimientos aplicables a este punto.

2.3. – Responsabilidad financiera

2.3.1 Responsabilidad Financiera del Certificador

No hay procedimientos aplicables a este punto.

2.4. - Interpretación y aplicación de las normas

2.4.1. - Legislación aplicable

El presente manual responden a la Ley 25.506, su decreto reglamentario N° 2628/02, la la Decisión Administrativa de la Jefatura de Gabinete de Ministros N° 06/2007 y demás normas aplicables.

El presente manual así como toda documentación asociada se actualizará cumpliendo los procedimientos que se detallan en el punto 8.- “Administración de Especificaciones”.

2.4.2. - Forma de interpretación y aplicación

La interpretación y/o aplicación del presente manual deberán seguir los lineamientos de la Política de Certificación correspondiente al presente Manual y demás documentos asociados, a la Ley 25.506, su Decreto reglamentario N° 2628/02, la Decisión Administrativa de la Jefatura de Gabinete de Ministros N° 06/2007, demás normas aplicables y de los procedimientos indicados en el punto 2.4.3.

2.4.3. - Procedimientos de resolución de conflictos

La resolución de conflictos que puedan suscitarse en la interpretación y/o aplicación de las disposiciones de el presente manual y/o en cualquiera de sus documentos asociados, ya sea entre los Suscriptores y la AFIP o terceros serán resueltos ajustándose a los procedimientos de la Ley 19.549, su decreto reglamentario 1759/72, y sus leyes modificatorias N° 21.686 y N° 25.344.

Tanto el suscriptor como los terceros usuarios podrán recurrir ante la Autoridad de Aplicación, previo agotamiento del procedimiento administrativo ante la AFIP.

2.5. – Aranceles

La AFIP se reserva el derecho de entregar en forma gratuita dispositivos criptográficos para soportar los certificados digitales de Clase 4, pero se reservará el derecho de requerir al suscriptor las garantías necesarias, a efectos de afianzar suficientemente el valor de mercado de dichos dispositivos, sin perjuicio de la gratuidad del servicio de otorgamiento de los certificados digitales.

2.6. - Publicación y Repositorios de certificados y listas de certificados revocados (CRLs)

2.6.1. - Publicación de información del certificador

La información detallada en el correspondiente punto de la Política de Certificación, está alojada dentro del sitio “acn.afip.gov.ar” accesible mediante internet. La publicación se realiza cumpliendo los procedimientos que se detallan en el punto 8.- “Administración de Especificaciones” del presente Manual de Procedimientos.

2.6.2. - Frecuencia de publicación

La lista de certificados revocados (CRL) y el repositorio de certificados se actualiza inmediatamente después de revocarse un certificado o emitirse uno, y en ningún caso superará una demora de 12 horas.

Independientemente de un suceso de revocación de un certificado, la lista de certificados revocados (CRL) se renueva cada 12 horas aunque no tuviere modificaciones.

Las actualizaciones al resto de la información contenida en el repositorio, se realizarán en un plazo menor a 24 horas, siempre que se hubiere cumplido con los procedimientos de Administración de Especificaciones del punto 8.- del presente manual.

2.6.3. - Controles de acceso a la información

El acceso permanente e irrestricto a la información publicada en su repositorio por parte de los suscriptores y terceros es monitoreado permanentemente por medio de un centro de control con guardia permanente, que detecta la indisponibilidad o falla del servicio de certificación, reportando el incidente al personal que en ese momento está consignado como guardia específica para la AC de la AFIP. Este último está

preparado y comprometido para actuar inmediatamente y resolver a la brevedad el inconveniente. En caso de resultar infructuoso en un tiempo acorde a la gravedad de la falla, se aplicará el Plan de Contingencias que corresponda al evento en trato.

2.6.4. – Repositorios de certificados y listas de revocación

La AC de la AFIP provee información del estado de validez de los certificados emitidos por medio de su sitio “acn.afip.gov.ar”, ingresando el número de certificado digital correspondiente, emitiendo el mensaje acorde.

El repositorio de certificados se actualiza inmediatamente después de ocurrida una emisión de un certificado digital.

Una vez determinada la necesidad de revocación de un certificado digital, el mismo se revoca inmediatamente por medio del Sistema Informático de AC de la AFIP.

La actualización de la lista de certificados digitales revocados se cumple en forma automática y sincrónica con la correspondiente operación de revocación del Sistema Informático de AC de la AFIP. Independientemente de ello, la lista se renueva cada 12 horas aunque no hubieran ocurrido novedades.

De este modo, salvo contingencias operativas, la publicación del estado de los certificados digitales revocados en el sitio web de la AC de la AFIP será de forma inmediata para su consulta por parte de terceros usuarios.

La lista de certificados digitales revocados incluye la fecha y la hora de la última actualización.

El acceso a la lista de certificados revocados es público, no estableciéndose ninguna clase de restricción. Se encuentra disponible en el sitio web de la AC de la AFIP “acn.afip.gov.ar/crl/afipacn.crl”, o bien se puede acceder al estado de los certificados por medio del servicio Online Certificate Status Protocol (OCSP) a través del sitio “acn.afip.gov.ar/ocsp/”.

El servicio OCSP debe configurarse en las aplicaciones cliente de los terceros usuarios, mediante la identificación de la autoridad certificante y la provisión de la URL del servicio.

2.7. – Auditorias

Para efectuar una auditoria sobre la AC de la AFIP, debe informarse al Responsable de la AC acerca del inicio de la misma, quien informará al Responsable de Seguridad, disponiendo los recursos para colaborar en la tarea.

El Responsable de Seguridad será en todo momento el responsable de atender los requerimientos de auditoria hasta la finalización de la misma.

2.8. – Confidencialidad

2.8.1. - Información confidencial

La divulgación de información considerada confidencial, a petición de autoridad judicial o competente, será autorizada en última instancia por el Responsable de la AC de la AFIP, quien decidirá sobre la conveniencia de la oportunidad y medio en que se realizará la comunicación del contenido al requirente.

2.8.2. - Información no confidencial

La información no confidencial que tenga que ver con la AC de la AFIP está accesible libremente desde Intranet en el sitio web “acn.afip.gov.ar”, en las secciones o repositorios correspondientes.

2.8.3. – Publicación de información sobre la revocación o suspensión de un certificado

El acceso a las listas de certificados revocados es público y esta disponible en el sitio web de la AC de la AFIP “acn.afip.gov.ar”, bajo los procedimientos especificados en el punto 2.6.4. – “Repositorios de certificados y listas de revocación” del presente Manual de Procedimientos.

De acuerdo con la ley 25.506, el estado de suspensión no está admitido.

2.8.4. – Divulgación de información a autoridades judiciales

Cuando existiese un pedido formal de información emanado de una Autoridad Judicial, sobre cualquiera de los datos o información de un suscriptor o grupo de ellos, incluyéndose expresamente pero no limitándose a la de “carácter confidencial”, se le dará el tratamiento detallado en el punto 2.8.1. – “Información confidencial” correspondiente al presente Manual de Procedimientos.

2.8.5. – Divulgación de información como parte de un proceso judicial o administrativo

Se aplicará idéntico procedimiento que el punto 2.8.4.- “Divulgación de información a autoridades judiciales”.

2.8.6. - Divulgación de información por solicitud del suscriptor

De acuerdo con la Ley 25326 de Protección de los Datos Personales, todo suscriptor de un certificado digital puede tener acceso a sus datos de identificación u otra información vinculada al ciclo de vida de su certificado digital. A esos efectos deberá efectuar la correspondiente solicitud por escrito ante su Puesto de Atención de la AR.

En caso que sea necesario divulgar información referida a los datos de identificación del suscriptor de un certificado digital, el suscriptor deberá otorgar la autorización correspondiente. La comunicación fehaciente al

suscriptor explicando los motivos del requerimiento deberá estar avalada por el Responsable de la AC de la AFIP, y podrá efectuarse por escrito o mediante una notificación desde el Portal de suscriptor de la AC de la AFIP.

2.8.7. – Otras circunstancias de divulgación de información

Cualquier otra circunstancia de divulgación de información no prevista en los apartados anteriores, será autorizada en última instancia por el Responsable de la AC de la AFIP, quien decidirá sobre la conveniencia de la oportunidad y medio en que se realizará la divulgación de la información en trato.

2.9. - Derechos de Propiedad Intelectual

El derecho de autor de los sistemas y aplicaciones informáticas desarrolladas por la AFIP para la implementación de su AC, así como de toda la documentación relacionada, pertenece a la AFIP. Los sistemas operativos y de soporte informático no desarrollados por la AFIP, cuentan con su respectiva licencia de uso.

El derecho de autor de la presente Política de Certificación y de toda otra documentación generada por la AFIP en relación con la infraestructura de firma digital, pertenece a la AFIP. Consecuentemente, dichos documentos no pueden ser reproducidos, copiados ni utilizados de ninguna manera, total o parcialmente, sin previo y formal consentimiento de la AFIP, de acuerdo a la legislación vigente acerca de los derechos de la propiedad intelectual.

Para solicitar autorización de uso o copia de los documentos y/o software de desarrollo propios de la AFIP, que están protegidos por el derecho de propiedad intelectual, dicha solicitud de autorización se debe presentar por escrito ante la Mesa de Entradas de la AC de la AFIP, dirigida al Responsable de la AC.

3- IDENTIFICACIÓN Y AUTENTICACIÓN

3.1. - Registro inicial

El solicitante de un certificado digital que será otorgado por la AC de la AFIP, debe ingresar al sitio web de la AC de la AFIP “acn.afip.gov.ar”, luego seleccionar la opción de “Gestionar certificados”, e iniciar una sesión por medio de su Clave Fiscal. Posicionado en el Portal del suscriptor, el solicitante debe identificarse y autenticarse en forma segura.

La Clave Fiscal es el método de autenticación de las personas físicas o jurídicas ante la AFIP, especificado por la Resolución General AFIP Nro. 2239/2007 y sus modificatorias posteriores.

Los niveles de seguridad asignados a la Clave Fiscal de AFIP determinan el grado de confiabilidad del procedimiento de validación de la identidad del poseedor, se describen en el Anexo II de la Resolución General AFIP Nro. 2239/2007 y los aplicables para solicitar certificados digitales son los siguientes:

- Nivel 3: Se tramita dirigiéndose a la dependencia de la AFIP (Agencia, Distrito, Aduana o Centro de Servicios) y presentando la documentación establecida por el Anexo II de la RG 2239 y modificatorias. Requiere verificación de identidad presencial.

- Nivel 4: Se tramita dirigiéndose a la Dependencia de la AFIP (Agencia, Distrito, Aduana o Centro de Servicios) y presentando la documentación establecida por el Anexo II de la RG AFIP 2239/2007 y modificatorias. Requiere verificación de identidad presencial y utilizar dispositivos de "hardware" de doble factor (un elemento físico y una contraseña o dato biométrico de activación como foto y/o huella dactilar) provistos u homologados por la AFIP.

3.1.1. - Tipos de Nombres

Para el CUIT/CUIL/CDI indicado en el punto 3.1.- “Registro inicial” del presente Manual de Procedimientos, la AC de la AFIP mostrará como nombre y apellido del solicitante aquellos obrantes en sus registros.

Si al momento de ingresar su solicitud el solicitante encontrara que el nombre o apellido mostrados por el sistema, no coincidieran con los de su documento de identidad, deberá ingresar los de éste último. En caso que tenga solicitudes de certificados en trámite, o certificados válidos, no podrá cambiarlos. La modificación de estos datos sólo impacta en el sistema de la AC de la AFIP.

Si tuviera que efectuar correcciones sobre su CUIL/CUIT/CDI, deberá efectuar los procedimientos indicados en el punto 3.1.5.- “Procedimiento de resolución de disputas sobre nombres” de este manual.

3.1.2.- Necesidad de Nombres Distintivos

No hay procedimientos aplicables a este punto.

3.1.3.- Reglas para la interpretación de nombres

El procedimiento de interpretación de nombres está implementado en el sistema informático de la AC de la AFIP, por medio de las rutinas adecuadas y desarrolladas al respecto. Las ambigüedades o conflictos que pudieran generarse cuando se usan caracteres especiales en los contenidos de los campos de información de certificados digitales se tratarán de modo de asegurar la compatibilidad de los datos almacenados en el certificado.

Respecto de la interpretación de ciertos caracteres especiales que pudieran estar presentes en el nombre o apellido del solicitante/suscriptor, éste último deberá reflejarlos de manera acorde a como están escritos en su documento de identificación personal.

3.1.4. - Unicidad de nombres

No hay procedimientos aplicables a este punto.

3.1.5.- Procedimiento de resolución de disputas sobre nombres

En la solicitud sólo se aceptarán números de CUIL/CUIT/CDI válidos para la emisión. En caso de conflictos el solicitante o suscriptor deberá solicitar la resolución del inconveniente ante el organismo responsable del nombre en cuestión: para el caso de un CUIL, la Administración Nacional de la Seguridad Social (ANSES), para el caso de un CUIT/CDI, deberá resolverlo ante una dependencia de la AFIP. El solicitante tiene la opción en el sistema informático de la AC, de corregir sus datos de nombre y apellido al momento de solicitar un certificado, corrección que tendrá efecto únicamente a los fines del certificado digital. La modificación de datos del padrón deberá realizarse por otra vía ante la autoridad que corresponda.

Para la resolución de disputas sobre nombres ante el caso de una incongruencia, error, omisión o duplicación de datos de identificador de usuario en el CUIL/CUIT/CDI del solicitante de un certificado digital, que no hayan podido ser resueltas efectivamente por los organismos administradores o responsables de esos datos, se podrá recurrir a la AC de la AFIP mediante la presentación de una nota en su Mesa de Entradas, dirigida al Responsable de la AC de la AFIP, explicando el caso. La AFIP evaluará en instancias administrativas la situación planteada.

3.1.6.- Reconocimiento, autenticación y rol de las marcas registradas

No se permite el uso de marcas comerciales, marcas de servicios o nombres de fantasía como nombres distintivos en los certificados de la AC de la AFIP

3.1.7. - Métodos para comprobar la posesión de la clave privada

En el caso de las solicitudes para certificados digitales Clase 3, el solicitante generará su par de claves usando su propio equipamiento al momento de la solicitud del certificado.

En el caso de las solicitudes para certificados digitales Clase 4, el solicitante generará su par de claves usando su propio dispositivo criptográfico en el Puesto de Atención.

Las claves criptográficas, en ambos casos, son generadas por el solicitante y no quedan almacenadas en el sistema informático de la AC de la AFIP. Luego el solicitante entregará su solicitud de certificado en formato PKCS#10, el cual no incluye la clave privada.

De esta forma queda garantizada la posesión de la clave privada exclusivamente por parte del solicitante o suscriptor.

El personal del Puesto de Atención se abstendrá de generar, exigir, tomar conocimiento o acceder bajo ninguna circunstancia a la clave privada del suscriptor.

3.1.8.- Autenticación de la identidad de personas jurídicas públicas o privadas

No hay procedimientos aplicables a este punto.

3.1.9. - Autenticación de la identidad de personas físicas

La verificación de la identidad de los solicitantes de los certificados de personas físicas se lleva a cabo mediante la contrastación de los datos de número, apellidos, nombres y foto obrantes en el documento de identidad válido que el solicitante debe presentar en el Puesto de Atención de la AR.

Para la verificación de la identidad y demás aspectos verificables se aplicarán las condiciones establecidas para el Nivel de Seguridad 3 y 4 de

Clave Fiscal, establecidos y descriptos por la Resolución General AFIP 2239/07 y modificatorias.

La mencionada Resolución General, en los puntos pertinentes a la verificación de identidad y demás aspectos verificables que se aplican a la presente Política de Certificación, establece que la documentación requerida al solicitante de un certificado digital es:

1.- Argentinos nativos o naturalizados y extranjeros: original y fotocopia del documento nacional de identidad, libreta cívica o libreta de enrolamiento. Los extranjeros deberán presentar el original y fotocopia del pasaporte o cédula del MERCOSUR (de tratarse de un país limítrofe de este bloque).

2.- Extranjeros con residencia en el país -incluida la temporaria o transitoria- que no posean documento nacional de identidad: original y fotocopia de la cédula de identidad, o del certificado o comprobante que acredite el número de expediente asignado por la Dirección Nacional de Migraciones, donde conste el carácter de su residencia.

El Oficial de Registro verificará que el documento presentado corresponda a la persona que lo exhibe.

El documento exhibido deberá estar en buen grado de conservación, y sus datos deberán ser concordantes con los obrantes en la solicitud. La foto deberá ser actual y reflejar concordancia con los aspectos físicos más característicos de la persona identificada.

Los Puestos de Atención de la AR conservarán la documentación de respaldo del proceso de verificación de identidad, inclusive aquella que no hubiera sido verificada durante este proceso, cumpliéndose las exigencias del Art. 21 Inc. f) e i) de la Ley 25.506 y el Art. 34 m) del Decreto 2628/02.

El suscriptor de un certificado firmará el formulario de adhesión al “Acuerdo con Suscriptor” que, entre otras, contiene la declaración de que la información que presentó para ser incluida en el certificado es correcta.

3.1.9.1.- Casos de no aprobación de una solicitud de certificado

Se indican a continuación los casos en que no se aprobará una solicitud de certificado digital.

a.- No es posible validar la identidad del solicitante

Si la identidad del solicitante no ha podido ser validada satisfactoriamente por medio de los procedimientos indicados para el alta de un certificado digital, el Oficial de Registro no debe aprobar la solicitud y se debe realizar lo siguiente:

a.1.- El Oficial de Registro debe informar al solicitante acerca de los elementos y/o pasos faltantes para finalizar satisfactoriamente el proceso de validación de su identidad.

a.2.- El solicitante tiene un plazo de treinta (30) días corridos a partir de la generación de la solicitud, para proveer la información faltante o complementaria que se le solicite.

a.3.- En caso de no completarse el trámite pasado dicho plazo, la solicitud será revocada automáticamente por el sistema de la AC de la AFIP y el solicitante debe reiniciar el proceso de solicitud de emisión del certificado digital, efectuando un nuevo requerimiento.

b.- El dispositivo criptográfico provisto por el solicitante no está homologado

Si el dispositivo criptográfico provisto por el solicitante no está aprobado por la AFIP, el Oficial de Registro no debe aprobar la solicitud y se debe realizar lo siguiente:

b.1.- El Oficial de Registro debe informar al solicitante que no es posible aprobar su solicitud debido a que el dispositivo criptográfico que pretende utilizar no está aprobado por la AFIP.

b.2.- El solicitante tiene un plazo de treinta (30) días corridos a partir de la generación de la solicitud, para presentarse nuevamente en el Puesto de Atención con un dispositivo criptográfico homologado por la AC de la AFIP, oportunidad en que deberá repetirse la verificación de identidad del solicitante.

b.3.- En caso de no completarse el trámite pasado dicho plazo, la solicitud será revocada automáticamente por el sistema de la AC de la AFIP y el solicitante debe reiniciar el proceso de solicitud de emisión del certificado, efectuando un nuevo requerimiento.

c.- Revocación de solicitud

En caso que una solicitud no sea aprobada en alguna de sus instancias en el término de treinta (30) días corridos desde su generación, caducará en forma automática por la ejecución de reglas internas del Sistema Informático de AC de la AFIP. El solicitante deberá realizar una nueva solicitud.

3.2.- Generación de nuevo par de claves (rutina de “Re Key”)

No está habilitada la generación de un nuevo par de claves para un certificado digital ya emitido. En caso de que por cualquier causa resultare necesario cambiar el par de claves, el suscriptor deberá solicitar la revocación de su certificado y la emisión de un nuevo certificado siguiendo los procedimientos previstos a este efecto.

3.3.- Generación de nuevo par de claves después de una revocación – Sin compromiso de clave

Luego de una revocación el suscriptor puede solicitar un nuevo certificado digital, siguiendo los procedimientos establecidos a ese efecto.

3.4. - Requerimiento de revocación

La AC de la AFIP admite y procesa solicitudes de revocación recibidas de los suscriptores o sus terceros autorizados. Los terceros autorizados se designan mediante el procedimiento previsto por medio del "Servicio de Delegación" de Clave Fiscal. Por medio del mismo se especifica a un tercero para que actúe en representación de su titular en los trámites habilitados para este Servicio de Delegación.

El titular de un certificado digital emitido por la AC de la AFIP, puede solicitar la revocación de un certificado digital del cual es suscriptor, mediante alguno de los siguientes procedimientos:

- Mediante su Clave Fiscal, ingresando al Portal de suscriptor,
- Por medio de la Mesa de Ayuda de la AC de la AFIP, con su Código de Revocación Telefónico,
- Por presentación personal en cualquier Puesto de Atención de la AR de la AFIP,
- Por medio de un tercero autorizado mediante el servicio de delegación con Clave Fiscal.

Además, la AFIP, sin requerimiento del suscriptor, puede determinar la revocación del certificado si detecta algún caso previsto en la Ley 25506, Art. 19 inc. e), o en el Decreto 2628/2002, Art. 23.

3.4.1 Revocación a solicitud del titular del certificado digital

El titular puede solicitar la revocación de un certificado digital mediante alguno de los siguientes procedimientos:

3.4.1.1.- Mediante Clave Fiscal

3.4.1.1.1.- Ingresar al Portal del suscriptor de la AC de la AFIP utilizando su Clave Fiscal, e ingresar en "Mis Certificados"

3.4.1.1.2.- Identificar el certificado digital a revocar y ejecutar la acción de "Revocar certificado digital".

3.4.1.1.3.- Indicar la causa de la revocación.

3.4.1.1.4.- Aceptar la operación.

3.4.1.2.- Por medio de la Mesa de Ayuda de la AC de la AFIP

Existe una Mesa de Ayuda disponible las 24 horas para este servicio de revocación de certificados digitales.

3.4.1.2.1.- Llamar telefónicamente a la Mesa de Ayuda: 0-810-999-2347

3.4.1.2.2.- Identificarse con CUIT/CUIL/CDI y optativamente indicar la identificación (nro. de serie) del certificado digital que desea revocar. Si no recuerda el número de serie y posee más de un certificado activo, la Mesa de Ayuda brindará indicios sobre los certificados existentes para poder individualizarlos (fechas, clase, etc.).

3.4.1.2.3.- El titular deberá informar el Código de Revocación Telefónico que tenga válido en ese momento (dicho código es el que eligió en el momento en que solicitó su primer certificado digital, o puede ser cambiado a voluntad desde el menú correspondiente en el Portal del suscriptor).

3.4.1.2.4.- Manifiestar su decisión de revocar el certificado digital indicando al operador telefónico las causas de la solicitud.

3.4.1.2.5.- El Operador de la Mesa de Ayuda de la AC de la AFIP deberá ejecutar la opción de "Revocación de Certificado Digital" del Sistema Informático de AC de la AFIP, con los datos que le fueron suministrados en los pasos anteriores, y firmar digitalmente la operación con su propio dispositivo criptográfico.

3.4.1.3.- Personalmente en un Puesto de Atención de la AR

3.4.1.3.1.- Presentarse personalmente en un Puesto de Atención de la AR de la AFIP dentro de los horarios de atención, informando sus datos y la identificación del certificado digital que desea revocar.

3.4.1.3.2.- El Oficial de Registro debe verificar la identidad del titular de acuerdo a la RESOLUCION GENERAL AFIP N° 2239/2007 y modificatorias para los niveles de seguridad 3 o 4.

3.4.1.3.3.- Manifiestar al Oficial de Registro las causas de la solicitud de revocación.

3.4.1.3.4.- El Oficial de Registro deberá ejecutar la opción de "Revocación de Certificado Digital" del Sistema Informático de AC de la AFIP, con los datos que le fueron suministrados en los pasos anteriores, y firmar digitalmente la operación con su propio dispositivo criptográfico.

3.4.1.4.- A través de un tercero autorizado

Se admite un pedido de revocación efectuado por un tercero, que fue autorizado previamente por el titular de un certificado. Para dicha autorización, el titular de un certificado debe ingresar al "Administrador de Relaciones" de la AFIP con su Clave Fiscal, elegir un tercero y autorizarlo para efectuar revocaciones de certificados.

El tercero debe aceptar dicha designación ingresando con su clave fiscal al servicio de "Aceptación de Designación". La próxima vez que ingrese al Portal de suscriptor de la AC, verá desplegadas en pantalla las opciones de identificación con la cual está habilitado para ingresar (la suya propia y su/s representado/s). En caso que opte por su representado verá un menú restringido del titular de los certificados, donde podrá identificar y revocar el/los certificado/s.

3.4.2 Revocación por parte de la AFIP

Al detectarse la presencia de algún causal de revocación por parte de la AFIP según la legislación vigente, el Responsable de la AR solicitará la revocación del o los certificados digitales que corresponda/n a los Puestos de Atención que designe.

3.4.2.1.- Revocación de un único certificado digital

3.4.2.1.1 - El Responsable de AR debe constatar que la causa de la revocación del certificado digital en cuestión esté dentro de las previstas por la política correspondiente al presente manual.

3.4.2.1.2 - El Responsable de AR debe solicitar por escrito la revocación a un Puesto de Atención, con los datos del titular y del certificado digital en cuestión, explicitando la causa.

3.4.2.2.- Revocación de múltiples certificados digitales

El Sistema Informático de la AC de la AFIP prevé medios para realizar revocaciones múltiples en caso de existir varios certificados digitales afectados por un mismo causal de revocación, para facilitar la tarea. Este tipo de revocaciones pueden ser solicitadas por el Responsable de AR al Responsable de la AC, quien por medio del Administrador de Servidores aplicará el mismo procedimiento que para el caso de un único certificado digital.

4. - CICLO DEL CERTIFICADO: REQUERIMIENTOS OPERATIVOS

4.1. - Solicitud de certificado

Todo potencial suscriptor de un certificado digital en los términos del presente documento (en adelante el “solicitante”) que desee obtener un certificado digital, debe iniciar el trámite de solicitud ingresando al sitio web de la AC de la AFIP “acn.afip.gov.ar” e ingresar al menú de “Gestione sus Certificados”, pudiendo realizar pedidos de dos tipos de certificados.

Los certificados digitales de suscriptor que emite la AFIP bajo la Política de Certificación que se corresponde con el presente Manual de Procedimientos, son de tres clases:

- Clase 3: Implementado por software.
- Clase 4: Implementado por medio de un dispositivo criptográfico.
- OCSP: El suscriptor es la AFIP, usado en relación con el servicio de verificación en línea del estado de un certificado.

La clase de certificado determina su posibilidad de uso y aplicabilidad en los sistemas que implementen la firma digital.

Los navegadores soportados por el Sistema Informático de AC de la AFIP en las estaciones de trabajo de los suscriptores son:

- Internet Explorer 6 o superior
- Firefox 1.0 o superior

4.1.1.- Requisitos para la solicitud de certificados digitales

Exceptuando el certificado OCSP, la AFIP únicamente emite certificados digitales para personas físicas que posean una Clave Fiscal de AFIP. Además se debe:

- Poseer como mínimo el nivel tres (3) de seguridad de autenticación en Clave Fiscal de la AFIP, de acuerdo a lo establecido en la Resolución General AFIP 2239/07. Dicho nivel mínimo requiere que el solicitante de un certificado digital se haya presentado personalmente en la delegación de la AFIP que corresponda a su domicilio fiscal, para verificar o asignar el mismo.
- Acceder al Portal de suscriptor mediante Clave Fiscal, para efectuar una solicitud de certificado de firma digital, consignando los datos que allí se soliciten.

- No poseer sanciones dictadas por autoridades competentes que impidan el otorgamiento de un certificado digital.
- Cumplir con lo establecido en la presente Política de Certificación, y demás documentos asociados en lo que tenga relación con la solicitud de certificado que se presenta.
- Cumplir con las condiciones establecidas en el “Acuerdo con Suscriptor” que habrá de firmar.

Según lo indicado precedentemente respecto de Clave Fiscal, la emisión de certificados digitales Clase 3 o Clase 4, requiere de verificación presencial de identidad.

Si el solicitante cumpliera las condiciones para recibir un dispositivo criptográfico provisto por la AC de la AFIP, el sistema informático le notificará tal circunstancia al realizar la solicitud y le indicará la lista de los Puestos de Atención de la AR de la AFIP en las cuales podría retirar el mencionado dispositivo y completar el trámite.

4.1.2.- Presentación de la solicitud

Se debe cumplir lo establecido en el Anexo II de la Resolución General AFIP Nro. 2239 y sus modificatorias posteriores, en lo referente a los niveles 3 y 4 de seguridad, según lo explicitado en el punto 3.1.9. – “Autenticación de la identidad de personas físicas” del presente Manual de Procedimientos, y adicionalmente la documentación que conforma el Acuerdo Tipo con Suscriptores, detallada en el anexo del presente Manual de Procedimientos. Dicha documentación es impresa desde el sistema con los datos consignados al momento de la solicitud.

Para cada Clase de Certificado, se deben cumplir los siguientes pasos:

4.1.2.1.- CLASE 3: certificado implementado por software.

En la estación de trabajo del solicitante:

PASO1: el sistema mostrará datos del solicitante o suscriptor, quien deberá verificarlos y confirmarlos para poder continuar con el trámite. Los datos incorrectos, podrán ser modificados directamente, solo en el caso que no tuviera un certificado en trámite o ya emitido, donde ya no podrá cambiarlos. Opcionalmente el solicitante o suscriptor puede ingresar una dirección de correo electrónico, para ser incluida en el certificado. Debe ingresar el “Código de Revocación Telefónico”, que será solicitado por la Mesa de Ayuda en caso de revocar telefónicamente un certificado. Finalizado este paso oprime la tecla enter e ingresa al siguiente paso.

PASO 2: el solicitante o suscriptor debe seleccionar el Puesto de Atención al cual desea concurrir para validar su identidad. Finalizado este paso oprime la tecla enter e ingresa al siguiente paso.

PASO 3: el solicitante o suscriptor debe seleccionar si desea generar la solicitud de certificado utilizando el navegador o por medio de un requerimiento en formato “PKCS#10” generado por otra aplicación. Si elige la opción de utilizar el navegador, en éste se generará el par de claves, y la clave privada queda bajo control del solicitante. Finalizado este paso oprime la tecla “enter” e ingresa al siguiente paso.

PASO 4: Si el solicitante o suscriptor seleccionó el navegador para la generación del par de claves, debe indicar el tamaño de clave (1024 o 2048 bits) y elegir el “Nivel de Seguridad” de la clave dentro del almacén de certificados. Se recomienda seleccionar nivel alto, es decir protegerla con una clave personal. Al aceptar esta ventana, luego de configurado el nivel de seguridad, el navegador creará y almacenará el par de claves criptográficas y transmitirá a la AC de la AFIP la solicitud del certificado. Finalizado este paso oprime la tecla enter e ingresa al siguiente paso.

PASO 5: el solicitante o suscriptor deberá descargar e imprimir el formulario de adhesión al “Acuerdo con Suscriptor”, que deberá

presentar ante el Puesto de Atención elegido. En este paso finaliza la solicitud desde la estación de trabajo del solicitante o suscriptor, para continuar luego en el Puesto de Atención. Mientras tanto, la solicitud del certificado queda pendiente de procesamiento en el sistema informático de la AC y asociada al Puesto de Atención mencionado.

4.1.2.2.-CLASE 4: certificado implementado en un dispositivo criptográfico.

En la estación de trabajo del solicitante:

PASO 1: el sistema mostrará en pantalla ciertos datos del solicitante, quien deberá verificarlos y confirmarlos para poder continuar con el trámite. Si dichos datos fueran incorrectos, podrá corregirlos directamente. Si tuviera un certificado en trámite o ya emitido, no podrá cambiarlos. Opcionalmente puede ingresar en el sistema una dirección de correo electrónico de contacto. Finalmente debe ingresar el Código de Revocación Telefónico, que es único por suscriptor, y servirá para revocar por parte del suscriptor, y por medio de la Mesa de Ayuda, el o los certificados activos, en caso de no recordar su Clave Fiscal o tener un impedimento en su uso. Si no recuerda el Código de Revocación Telefónico, debe establecer uno nuevo por medio del ítem de menú correspondiente, respetando las reglas de selección indicadas por el sistema.

PASO 2: debe seleccionar el Puesto de Atención al cual desea concurrir para certificar su identidad.

PASO 3: deberá descargar e imprimir los formularios de adhesión al “Acuerdo con Suscriptor”, que deberá presentar personalmente ante el Puesto de Atención elegido. Mientras tanto, su pedido queda pendiente de procesamiento en el sistema informático de la AC y asociado al Puesto de Atención mencionado.

4.1.3.- Aprobación de la solicitud

El Oficial de Registro evaluará la solicitud de certificado, verificando la identidad del solicitante en forma presencial y demás datos pertinentes, y en caso de corresponder dará curso favorable a la solicitud.

Una vez admitida la solicitud de Clase 3, el Oficial de Registro efectuará la verificación de identidad del solicitante y recibirá el formulario de adhesión al “Acuerdo con Suscriptor” firmado por éste. Luego aprobará la solicitud y le entregará el “Código de Activación” del certificado digital que el suscriptor deberá conservar para utilizarlo en la aceptación del certificado.

Una vez admitida la solicitud de Clase 4, el Oficial Certificador efectuará la verificación de identidad, constatará que el dispositivo criptográfico sea el homologado en caso que sea provisto por el solicitante y recibirá el formulario de adhesión al “Acuerdo con Suscriptor”. Luego pre-aprobará la solicitud. Si el dispositivo es provisto por la AFIP, el Oficial Certificador imprimirá el correspondiente recibo en el cual constarán los datos de la unidad a entregar con sus correspondientes instructivos y software, y el solicitante deberá conformarlo.

4.1.4.- Generación del par de claves criptográficas del suscriptor

La generación del par de claves criptográficas del suscriptor depende de la clase de certificado solicitada.

En el caso de un certificado digital Clase 3, el solicitante, debe cumplir los siguientes pasos:

PASO 3: el solicitante o suscriptor debe seleccionar si desea generar la solicitud de certificado utilizando el navegador o por medio de un requerimiento en formato “PKCS#10” generado por otra aplicación. Si elige la opción de utilizar el navegador, en éste se generará el par de claves, y la clave privada queda bajo control del solicitante. Finalizado este paso oprime la tecla enter e ingresa al siguiente paso.

PASO 4: Si el solicitante o suscriptor seleccionó el navegador para la generación del par de claves, debe indicar el tamaño de clave (1024 o 2048 bits) y elegir el “Nivel de Seguridad” de la clave dentro del almacén de certificados. Se recomienda seleccionar nivel alto, es decir protegerla con una clave personal. Al aceptar esta ventana, luego de configurado el nivel de seguridad, el navegador creará y almacenará el par de claves criptográficas y transmitirá a la AC de la AFIP la solicitud del certificado. Finalizado este paso oprime la tecla enter e ingresa al siguiente paso.

En el caso de un certificado digital Clase 4, el solicitante, continuando en el Puesto de Atención, con la presencia del Oficial de Registro verificando la utilización del dispositivo homologado, debe ingresar mediante su Clave Fiscal al “Portal de solicitante o suscriptor”, identificar la solicitud de certificado ya aprobada en el menú de “Mis Trámites”, indicada como “Pendiente de generación de Claves Criptográficas”, y “Verla”. Luego debe seleccionar la opción de generar las claves y continuar con los siguientes pasos:

PASO 5: Debe conectar el dispositivo criptográfico a un puerto USB de dicha estación de trabajo y hacer click en “Continuar”. Debe seleccionar el proveedor de servicios criptográficos que corresponda. Si el dispositivo criptográfico es el provisto por la AFIP debe cambiarle la clave de protección mediante la utilidad de cambio de clave. Debe seleccionar la longitud de la clave y luego “Generar”. Aceptar el cartel de alerta de “Peligro potencial...” (sólo en caso del navegador de Internet Microsoft Explorer), aceptar el aviso de acceso al dispositivo criptográfico y luego ingresar la clave del mismo en la ventana emergente. La operación demora unos momentos. Una vez finalizada debe retirar su dispositivo y cerrar su sesión.

4.1.5.- Solicitud de renovación del Certificado

Un suscriptor puede solicitar la renovación de su certificado digital dentro de su período de validez, con un máximo de 2 (dos) renovaciones desde la

emisión del certificado digital original. El suscriptor entiende que este proceso de renovación no debe aplicarse cuando se deba cambiar algún dato del certificado a renovar. La renovación de un certificado digital de suscriptor no implica generar un nuevo par de claves. Transcurrido el período de validez del par de claves asociadas al certificado, el certificado digital asociado no podrá renovarse y dichas claves no deberán ser usadas por el suscriptor, de acuerdo a lo indicado en el punto 6.3.2 de la presente Política de Certificación.

El sistema informático de la AC de la AFIP, colocará un mensaje en el Portal del suscriptor treinta (30) días antes de vencimiento del certificado, y adicionalmente enviará un mail desde la cuenta "acn@afip.gov.ar" a la dirección que el suscriptor tenga consignada en el sistema.

Para el caso de certificados digitales de Clase 3, el procedimiento es ingresar al sistema de la AC de la AFIP, iniciar sesión mediante su Clave Fiscal, ingresar al menú de "Mis Certificados", identificar el certificado a renovar y efectuar la acción de renovación. El botón de acción para la renovación aparecerá automáticamente a partir del momento en que resten 30 días para su vencimiento. Una vez concluida exitosamente, deberá importar el nuevo certificado a su estación de trabajo.

Para el caso de certificados digitales de Clase 4, el procedimiento es similar.

4.2. - Emisión del certificado

4.2.1.- Proceso de emisión de certificado digital de Clase 3

4.2.1.1.- Antes de los 30 días corridos a partir de la creación de la solicitud, el solicitante se debe presentar con la documentación requerida en el Puesto de Atención que eligió, donde se debe efectuar la verificación de identidad. De resultar satisfactoria, el Oficial de Registro debe ingresar al módulo de AR del Sistema Informático de AC de la AFIP, iniciando sesión mediante su Clave Fiscal, y luego con su propio dispositivo criptográfico

debe aprobar la solicitud. De no resultar satisfactoria la verificación de identidad del solicitante, se debe aplicar el procedimiento 3.1.9.1.- “Casos de no aprobación de una solicitud de certificado”.

4.2.1.2. Una vez aprobada su solicitud, el Oficial de Registro le entregará el código de activación del certificado digital y el solicitante se retirará del Puesto de Atención de la AR, quedando a la espera de la emisión del correspondiente certificado digital por parte de la AC de la AFIP.

4.2.2.- Proceso de emisión de certificado digital de Clase 4

4.2.2.1.- Antes de 30 días corridos a partir de la creación de la solicitud, el solicitante se debe presentar con la documentación requerida en el Puesto de Atención que eligió, donde se debe efectuar la verificación de identidad. De resultar satisfactoria, el Oficial de Registro debe ingresar, mediante su Clave Fiscal, al módulo de AR del Sistema Informático de AC de la AFIP, y con su propio dispositivo criptográfico debe pre-aprobar la solicitud. De no resultar satisfactoria la verificación de identidad, se debe aplicar el procedimiento 3.1.9.1.- “Casos de no aprobación de una solicitud de certificado”.

4.2.2.2.- El Oficial de Registro será notificado por el módulo de AR del Sistema Informático de AC de la AFIP si el solicitante fue seleccionado para recibir un dispositivo criptográfico por parte de la AC de la AFIP, en cuyo caso procederá a ejecutar la opción "Entrega de dispositivo criptográfico" de dicho sistema, imprimir el correspondiente recibo en el cual constarán los datos de la unidad a entregar y requerir al solicitante que firme dicho recibo en su presencia. Le entregará el dispositivo criptográfico inicializado junto con la correspondiente clave de protección.

4.2.2.3.- Si el solicitante optó por traer su propio dispositivo criptográfico, el Oficial de Registro deberá verificar, mediante la herramienta de verificación de su módulo de AR, que el mismo se corresponde con alguno de los modelos homologados por la AFIP, debiendo en caso contrario aplicar el

procedimiento 3.1.9.1.- “Casos de no aprobación de una solicitud de certificado”.

4.2.2.4.- Continuando en el Puesto de Atención, el solicitante, con la presencia del Oficial de Registro verificando el uso del dispositivo homologado, debe ingresar al Portal del Solicitante/suscriptor, identificar la solicitud de certificado ya aprobada en el menú de “Mis Trámites”, y seleccionar la opción de generar las claves. Debe conectar el dispositivo criptográfico a un puerto USB de dicha estación de trabajo, si es el provisto por la AFIP debe cambiarle la clave de protección mediante la utilidad de cambio de clave, e indicar en el sistema de la AC que genere el par de claves. Deberá ingresar la clave del dispositivo criptográfico cuando el sistema la solicite. Si el dispositivo criptográfico falla y no es posible realizar la importación, se debe aplicar el procedimiento 3.1.9.1.- “Casos de no aprobación de una solicitud de certificado”.

4.2.2.5.- El Oficial de Registro debe aprobar la emisión del certificado desde su Portal de AR firmando la solicitud, y entregar el código de aceptación de certificado al solicitante.

4.3. - Aceptación del certificado

La aceptación del certificado se cumple según sea la clase del certificado, Clase 3 o Clase 4. Si el Código de Aceptación no es recordado por el solicitante, podrá requerirlo nuevamente al mismo Oficial de Registro que le aprobó la solicitud.

4.3.1.- Aceptación de certificado digital de Clase 3

El solicitante debe ingresar al “Portal de suscriptor o solicitante”, ir a la opción “Mis Trámites”, identificar su solicitud de certificado y aceptarla, ingresando el Código de Activación que le fuera entregado en el Puesto de Atención. Podrá importar el certificado digital desde el menú de “Mis Certificados”, mediante la opción de “Importarlo mediante el navegador”.

Luego debe “Abrir” el certificado, “Instalar certificado”, hacer click dos veces en “Siguiente”, luego “Finalizar”, y luego “Aceptar” 2 veces más.

Si la solicitud hubiera sido realizada generando el par de claves en un determinado navegador, la aceptación y retiro del certificado digital debe ser realizada desde el mismo navegador. Si en cambio la solicitud hubiera sido realizada mediante un requerimiento “PKCS#10”, la aceptación y retiro del certificado digital pueden ser realizadas desde cualquier navegador soportado. Si el proceso no es exitoso, el mensaje mostrado indicará el origen del inconveniente y sugerirá la acción correctiva a tomar.

Si el solicitante no acepta explícitamente o no retira su certificado digital dentro de los treinta (30) días corridos desde su emisión, se procederá a su revocación en forma automática.

El suscriptor puede probar su certificado, firmando un texto con cualquier aplicación compatible disponible en su estación de trabajo.

4.3.2.- Aceptación de certificado digital de Clase 4

El solicitante debe volver a ingresar al “Portal de solicitante o suscriptor” y a conectar su dispositivo criptográfico a la estación de trabajo, ir al menú de “Mis Trámites”, identificar la solicitud (indicada como “Procesada. Pendiente de aceptación por parte del suscriptor”), y al “Verla” aceptar el certificado ingresando su Código de Activación. Luego debe importar el certificado mediante el botón de acción “Importar mediante el navegador”. Seleccionar “Abrir” en la ventana de descarga, “Instalar certificado”, “Siguiente”, confirmar la opción de “Selección automática de almacén”, luego “Siguiente” y “Finalizar”. Ingresar la clave del dispositivo criptográfico y finalmente “Aceptar”.

El suscriptor puede probar su dispositivo, firmando un texto de prueba disponible en el Portal de la AC.

En cualquier caso en que la importación de un certificado digital al dispositivo criptográfico no sea satisfactoria, o en el caso que el solicitante deba recibir por parte de la AFIP un dispositivo criptográfico y que por cualquier circunstancia no se disponga de alguno en el Puesto de Atención, mientras se cumpla el plazo de validez de la solicitud, podrá repetirse el proceso de importación. Pasado el mismo, deberá realizarse una nueva solicitud.

4.4. - Suspensión y Revocación de Certificados

4.4.1. - Causas de revocación

No hay procedimientos aplicables a este punto.

4.4.2. - Autorizados a solicitar la revocación.

No hay procedimientos aplicables a este punto.

4.4.3.- Procedimientos para la solicitud de revocación

Se detallan en el punto 3.4.- “Requerimiento de revocación” del presente Manual de Procedimientos.

4.4.4. - Plazo para la solicitud de revocación

No hay procedimientos aplicables a este punto.

4.4.5. – Causas de suspensión

No hay procedimientos aplicables a este punto.

4.4.6. – Autorizados a solicitar la suspensión

No hay procedimientos aplicables a este punto.

4.4.7. – Procedimientos para la solicitud de suspensión

No hay procedimientos aplicables a este punto.

4.4.8. – Límites del período de suspensión del certificado

No hay procedimientos aplicables a este punto.

4.4.9. - Frecuencia de emisión de listas de certificados revocados

La AFIP mantiene a disposición la lista de certificados revocados en forma permanente. La actualización de la CRL es cada 12 horas.

4.4.10. - Requisitos para la verificación de la lista de certificados revocados.

Para efectuar una verificación sobre un documento que hubiere sido firmado por un suscriptor de un certificado digital de la AC de la AFIP, se debe:

- Verificar que el certificado digital correspondiente al documento firmado, no se encuentre incluido en la lista de certificados revocados, proveyendo el número de certificado digital.
- Asegurar la autenticidad de la lista de certificados revocados, mediante la verificación de la firma digital de la AFIP que la emite y de su período de validez.

4.4.11. - Disponibilidad del servicio de consulta sobre revocación y de estado del certificado.

No hay procedimientos aplicables a este punto.

4.4.12. - Requisitos para la verificación en línea del estado de revocación

Se detallan en el punto 2.6.4. – “Repositorios de certificados y listas de revocación” del presente Manual de Procedimientos.

4.4.13. - Otras formas disponibles para la divulgación de la revocación

No hay procedimientos aplicables a este punto.

4.4.14. - Requisitos para la verificación de otras formas de divulgación de revocación

No hay procedimientos aplicables a este punto.

4.4.15. - Requisitos específicos para casos de compromiso de claves

Para solicitar la inmediata revocación de un certificado digital en caso de compromiso de claves, se debe realizar el pedido conforme el punto 3.4.1- “Revocación a solicitud del titular del certificado digital” del presente Manual de Procedimientos.

4.5. - Procedimientos de auditoría de seguridad

CONFIDENCIAL

4.5.1.- Generación y mantenimiento de archivos de auditoria

CONFIDENCIAL

4.5.1.1.- Eventos registrables

CONFIDENCIAL

4.5.2.- Copias de resguardo de archivos de transacciones de auditoría

CONFIDENCIAL

4.6. - Archivo de registros de eventos

CONFIDENCIAL

4.7. - Cambio de claves criptográficas de la AC de la AFIP

CONFIDENCIAL

4.8. - Plan de contingencia y recuperación ante desastres

CONFIDENCIAL

4.9. - Plan de Cese de Actividades

CONFIDENCIAL

5. - CONTROLES DE SEGURIDAD FÍSICA, FUNCIONALES Y PERSONALES

5.1.- Controles de Seguridad Física

CONFIDENCIAL

5.1.1.- Construcción y ubicación de instalaciones

CONFIDENCIAL

5.1.2.- Niveles de acceso físico

CONFIDENCIAL

5.1.3.- Energía y aire acondicionado

CONFIDENCIAL

5.1.4.- Exposición al agua

CONFIDENCIAL

5.1.5.- Prevención y protección contra incendios

CONFIDENCIAL

5.1.6.- Medios de almacenamiento

CONFIDENCIAL

5.1.7.- Disposición de material de descarte

CONFIDENCIAL

5.1.8.- Sitio alternativo

CONFIDENCIAL

5.1.9.- Sensores presenciales y de ambiente de la sala de la AC

CONFIDENCIAL

5.2. - Controles Funcionales

5.2.1.- Roles

CONFIDENCIAL

5.2.2.- Correspondencia roles – llaves del HSM.

CONFIDENCIAL

5.2.3.- Roles – Altas y modificaciones de roles

CONFIDENCIAL

5.2.4.- Roles - Cese de funciones – Reemplazo

CONFIDENCIAL

5.3. - Controles de Seguridad del Personal

CONFIDENCIAL

6. - CONTROLES DE SEGURIDAD TÉCNICA

6.1. - Generación e instalación de claves

6.1.1. - Generación del par de claves criptográficas

CONFIDENCIAL

6.1.2. - Entrega de la clave privada al suscriptor

CONFIDENCIAL

6.1.3. - Entrega de la clave pública al emisor del certificado

CONFIDENCIAL

6.1.4. - Disponibilidad de la clave pública del certificador

CONFIDENCIAL

6.1.5. - Tamaño de claves

CONFIDENCIAL

6.1.6. - Generación de parámetros de claves asimétricas

CONFIDENCIAL

6.1.7. - Verificación de calidad de los parámetros

CONFIDENCIAL

6.1.8. - Generación de claves por hardware o software

CONFIDENCIAL

6.1.9.- Propósitos de utilización de claves (campo “Key Usage” en certificados X.509 v.3)

CONFIDENCIAL

6.2. - Protección de la clave privada.

6.2.1. - Estándares para dispositivos criptográficos

CONFIDENCIAL

6.2.2. - Control “M de N” de clave privada

CONFIDENCIAL

6.2.3. - Recuperación de clave privada

CONFIDENCIAL

6.2.4. - Copia de seguridad de clave privada

CONFIDENCIAL

6.2.5. - Archivo de clave privada

CONFIDENCIAL

6.2.6. - Incorporación de claves privadas en dispositivos criptográficos

CONFIDENCIAL

6.2.7. - Método de activación de claves privadas

CONFIDENCIAL

6.2.8. - Método de desactivación de claves privadas

CONFIDENCIAL

6.2.9. - Método de destrucción de claves privadas

CONFIDENCIAL

6.3. - Otros aspectos de administración de claves

6.3.1.- Archivo permanente de la clave pública

CONFIDENCIAL

6.3.2. - Período de uso de clave pública y privada

CONFIDENCIAL

6.4. - Datos de activación

6.4.1.- Generación e instalación de datos de activación

CONFIDENCIAL

6.4.2. - Protección de los datos de activación

CONFIDENCIAL

6.4.3. – Otros aspectos referidos a los datos de activación

CONFIDENCIAL

6.5. - Controles de seguridad informática

6.5.1.- Requisitos Técnicos específicos

CONFIDENCIAL

6.5.2.- Calificaciones de seguridad computacional

CONFIDENCIAL

6.6. - Controles Técnicos del ciclo de vida de los sistemas

6.6.1. - Controles de desarrollo de sistemas

CONFIDENCIAL

6.6.2. – Administración de controles y seguridad

CONFIDENCIAL

6.6.3. - Calificaciones de seguridad del ciclo de vida del software

CONFIDENCIAL

6.7. - Controles de seguridad de red

CONFIDENCIAL

6.8. - Controles de ingeniería de dispositivos criptográficos

CONFIDENCIAL

7. - PERFILES DE CERTIFICADOS Y DE LISTAS DE CERTIFICADOS REVOCADOS

7.1. - Perfil del certificado

CONFIDENCIAL

7.2. - Perfil de la lista de certificados revocados

CONFIDENCIAL

7.3. - Perfil del certificado OCSP

CONFIDENCIAL

8. - ADMINISTRACIÓN DE ESPECIFICACIONES

8.1. - Procedimientos de cambio de especificaciones

CONFIDENCIAL

8.2. - Procedimientos de publicación y notificación

CONFIDENCIAL

8.3. - Procedimientos de aprobación

CONFIDENCIAL