ADMINISTRACIÓN FEDERAL DE INGRESOS PÚBLICOS

AUTORIDAD CERTIFICANTE

POLÍTICA DE CERTIFICACIÓN

OID: 2.16.32.1.1.1

Versión 2 – 16/06/2014

ÍNDICE

1. - INTRODUCCIÓN

1.1– Descripción general

El presente documento establece las políticas que se aplican a las relaciones entre la Administración Federal de Ingresos Públicos, los solicitantes y suscriptores de los certificados digitales emitidos por la Autoridad Certificante de la AFIP (en adelante AC de la AFIP) y los terceros usuarios de dichos certificados.

La autoridad de aplicación de firma digital en la República Argentina es la Secretaría de Gabinete y Coordinación Administrativa de la Jefatura de Gabinete de Ministros, en adelante “Autoridad de Aplicación”.

En este documento, todas las referencias al suscriptor de un certificado digital provisto por la AC de la AFIP, se entenderán también válidas para el solicitante en proceso de obtener un certificado digital, en la medida en que sean aplicables.

1.2. - Identificación

Nombre: Política de Certificación de la AC de la AFIP
Versión: 2
Fecha: _____
Sitio web: “acn.afip.gov.ar/cps/”
OID: 2.16.32.1.1.1
Lugar: Buenos Aires, Argentina

1.3. - Participantes y aplicabilidad

1.3.1. – Certificador

El Certificador es la Administración Federal de Ingresos Públicos (AFIP).

1.3.2. - Autoridad de Registro (AR)

Existe una única Autoridad de Registro enmarcada en el ámbito de aplicación de esta Política de Certificación, que posee Puestos de Atención establecidos por ella y conformados por áreas de la estructura organizativa de la AFIP.

Los Puestos de Atención se habilitan o deshabilitan de acuerdo al plan establecido por el Responsable de la AR y se publican junto con su dirección en el sitio web “acn.afip.gov.ar”, informándose dicha situación a la Autoridad de Aplicación.

1.3.3. - Suscriptores de certificados

Podrán suscribir los certificados digitales emitidos por la AC de la AFIP las personas físicas que utilizan los servicios de la AFIP mediante Clave Fiscal, y siempre que cumplan todos los requisitos expuestos en la presente política.

Además, la AFIP será suscriptora de un certificado, para ser usado en relación con el servicio OCSP de consultas sobre el estado de un certificado.

1.3.4. - Aplicabilidad

Los certificados emitidos por la AC de la AFIP bajo la presente Política de Certificación, tienen como objeto verificar la autenticidad e integridad de:

a) los documentos electrónicos de carácter tributario, aduanero, fiscal, administrativo y del comercio exterior firmados digitalmente que se intercambien entre los contribuyentes y la AFIP;
b) los documentos electrónicos de carácter tributario, fiscal y administrativo firmados digitalmente que se intercambien entre los contribuyentes y los organismos recaudadores provinciales y municipales, que adopten la utilización de certificados digitales emitidos por la AC de AFIP para sus sistemas de información;

c) los documentos firmados digitalmente presentados por personas físicas ante organismos de la Administración Pública Nacional, que adopten la utilización de certificados digitales emitidos por la AC de AFIP para sus sistemas de información.

d) las respuestas a las consultas sobre el estado de un certificado, por medio del servicio de verificación en línea del estado de los certificados, denominado Online Certificate Status Protocol (OCSP) o Protocolo en Línea del Estado de los Certificados.

El listado de organismos referidos en los puntos b) y c) puede accederse a través del sitio web “acn.afip.gov.ar/conv_organismos”.

Existen tres clases de certificados digitales contemplados bajo la presente Política:

a) Clase 3: Implementado por medio de software.

b) Clase 4: Implementado por medio de un dispositivo criptográfico.

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

1.4. - Contactos

Esta política es administrada 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 DE LA POLÍTICA DE CERTIFICACIÓN

2.1. – Obligaciones

2.1.1. - Obligaciones del certificador

Las obligaciones de la AFIP en su carácter de certificador licenciado se originan en la ley 25506, el decreto 2628/2002 y lo establecido por la AFIP a los efectos de esta política de certificación. La parte pertinente de esas normas es transcripta a continuación, con las modificaciones contenidas en normas complementarias posteriores.

2.1.1.1.- Obligaciones impuestas por la ley 25506, artículo 21:

a) Informar a quien solicita un certificado con carácter previo a su emisión y utilizando un medio de comunicación las condiciones precisas de utilización del certificado digital, sus características y efectos, la existencia de un sistema de licenciamiento y los procedimientos, forma que garantiza su posible responsabilidad patrimonial y los efectos de la revocación de su propio certificado digital y de la licencia que le otorga la Autoridad de Aplicación. Esa información deberá estar libremente accesible en lenguaje fácilmente comprensible. La parte pertinente de dicha información estará también disponible para terceros;

b) Abstenerse de generar, exigir, o por cualquier otro medio tomar conocimiento o acceder bajo ninguna circunstancia, a los datos de creación de firma digital de los titulares de certificados digitales por él emitidos;

c) Mantener el control exclusivo de sus propios datos de creación de firma digital e impedir su divulgación;

d) Operar utilizando un sistema técnicamente confiable de acuerdo con lo que determine la autoridad de aplicación;

e) Notificar al solicitante las medidas que está obligado a adoptar para crear firmas digitales seguras y para su verificación confiable, y las obligaciones que asume por el solo hecho de ser titular de un certificado digital;

f) Recabar únicamente aquellos datos personales del titular del certificado digital que sean necesarios para su emisión, quedando el solicitante en libertad de proveer información adicional;

g) Mantener la confidencialidad de toda información que no figure en el certificado digital;

h) Poner a disposición del solicitante de un certificado digital toda la información relativa a su tramitación;

i) Mantener la documentación respaldatoria de los certificados digitales emitidos, por diez (10) años a partir de su fecha de vencimiento o revocación;

j) Incorporar en su política de certificación los efectos de la revocación de su propio certificado digital y/o de la licencia que le otorgara la autoridad de aplicación;

k) Publicar en Internet o en la red de acceso público de transmisión o difusión de datos que la sustituya en el futuro, en forma permanente e ininterrumpida, la lista de certificados digitales revocados, las políticas de certificación, la información relevante de los informes de la última auditoría de que hubiera sido objeto, su manual de procedimientos y toda información que determine la autoridad de aplicación;

l) Publicar en el Boletín Oficial aquellos datos que la autoridad de aplicación determine;

m) Registrar las presentaciones que le sean formuladas, así como el trámite conferido a cada una de ellas;

n) Informar en las políticas de certificación si los certificados digitales por él emitidos requieren la verificación de la identidad del titular;

o) Verificar, de acuerdo con lo dispuesto en su manual de procedimientos, toda otra información que deba ser objeto de verificación, la que debe figurar en las políticas de certificación y en los certificados digitales;

p) Solicitar inmediatamente la Autoridad de Aplicación la revocación de su certificado, o informarle la revocación del mismo, cuando existieren indicios de que los datos de creación de firma digital que utiliza hubiesen sido comprometidos o cuando el uso de los procedimientos de aplicación de los datos de verificación de firma digital en él contenidos hayan dejado de ser seguros;

q) Informar inmediatamente la Autoridad de Aplicación sobre cualquier cambio en los datos relativos a su licencia;

r) Permitir el ingreso de los funcionarios autorizados de la Autoridad de Aplicación o de los auditores a su local operativo, poner a su disposición toda la información necesaria y proveer la asistencia del caso;

s) Emplear personal idóneo que tenga los conocimientos específicos, la experiencia necesaria para proveer los servicios ofrecidos y en particular, competencia en materia de gestión, conocimientos técnicos en el ámbito de la firma digital y experiencia adecuada en los procedimientos de seguridad pertinentes;

t) Someter a aprobación de la Autoridad de Aplicación el Manual de Procedimientos, el Plan de Seguridad y el de Cese de Actividades, así como el detalle de los componentes técnicos a utilizar;

u) Constituir domicilio legal en la República Argentina;

v) Disponer de recursos humanos y tecnológicos suficientes para operar de acuerdo a las exigencias establecidas en la presente ley y su reglamentación;

w) Cumplir con toda otra obligación emergente de su calidad de titular de la licencia adjudicada por la Autoridad de Aplicación.

2.1.1.2.- Obligaciones impuestas por el decreto 2628/2002, artículo 34

Obligaciones del certificador licenciado. Además de lo previsto en el artículo 21 de la Ley N° 25.506, los certificadores licenciados deberán:

a) Comprobar por sí o por medio de una Autoridad de Registro que actúe en nombre y por cuenta suya, la identidad y cualquier otro dato de los solicitantes considerado relevante para los procedimientos de verificación de identidad previos a la emisión del certificado digital, según la Política de Certificación bajo la cual se solicita.

b) Mantener a disposición permanente del público las Políticas de Certificación y el Manual de Procedimientos correspondiente.

c) Cumplir cabalmente con las políticas de certificación acordadas con el titular y con su Manual de Procedimientos.

d) Garantizar la prestación establecida según los niveles definidos en el acuerdo de servicios pactados con sus usuarios, relativo a los servicios para los cuales solicitó el licenciamiento.

e) Informar al solicitante de un certificado digital, en un lenguaje claro y accesible, en idioma nacional, respecto de las características del certificado solicitado, las limitaciones a la responsabilidad, si las hubiere, los precios de los servicios de certificación, uso, administración y otros asociados, incluyendo cargos adicionales y formas de pago, los niveles de servicio al proveer, las obligaciones que el suscriptor asume como usuario del servicio de certificación, su domicilio en la República Argentina y los medios a los que el suscriptor puede acudir para solicitar aclaraciones, dar cuenta del mal funcionamiento del sistema o presentar sus reclamos.

f) Disponer de un servicio de atención a titulares y terceros, que permita evacuar las consultas y la pronta solicitud de revocación de certificados.

g) Garantizar el acceso permanente, eficiente y gratuito de los titulares y terceros al repositorio de certificados revocados.

h) Mantener actualizados los repositorios de certificados revocados por el período establecido por el Ente Administrador.

i) Abstenerse de generar, exigir, tomar conocimiento o acceder bajo ninguna circunstancia a la clave privada del suscriptor.

j) Informar a la Autoridad de Aplicación de modo inmediato la ocurrencia de cualquier evento que comprometa la correcta prestación del servicio.

k) Respetar el derecho del titular del certificado digital a no recibir publicidad de ningún tipo por su intermedio, salvo consentimiento expreso de éste.

l) Publicar en el Boletín Oficial durante UN (1) día, el certificado de clave pública correspondiente a la política para la cual obtuvo licenciamiento;

m) Cumplir las normas y recaudos establecidos para la protección de datos personales.

n) En los casos de revocación de certificados contemplados en el apartado 3 del inciso e) del artículo 19 de la Ley N° 25.506, deberá sustituir en forma gratuita aquel certificado digital que ha dejado de ser seguro por otro que sí cumpla con estos requisitos.

La Autoridad de Aplicación deberá establecer el proceso de reemplazo de certificados en estos casos. En los casos en los que un certificado

digital haya dejado de ser seguro por razones atribuibles a su titular, el certificador licenciado no estará obligado a sustituir el certificado digital.

o) Enviar periódicamente a la Autoridad de Aplicación, informes de estado de operaciones con carácter de declaración jurada.

p) Contar con personal idóneo y confiable, con antecedentes profesionales acordes a la función desempeñada.

q) Responder a los pedidos de informes por parte de un tercero respecto de la validez y alcance de un certificado digital emitido por él.

2.1.1.3.- Obligaciones adicionales y aclaraciones

La AFIP sustituirá en forma gratuita los certificados de suscriptores que hubieran sido revocados por haberse determinado que los procedimientos de emisión y/o verificación han dejado de ser seguros, de acuerdo con lo previsto en la ley 25506, artículo 19, inciso e), apartado 3. En esos casos el suscriptor deberá solicitar el reemplazo de su certificado digital de acuerdo con el procedimiento que determine la AFIP. En los casos en los que un certificado digital haya dejado de ser seguro por razones atribuibles a su titular, la AFIP no estará obligada a entregar un nuevo certificado digital.

2.1.2. - Obligaciones de la Autoridad de Registro

Las obligaciones de la Autoridad de Registro se originan en el decreto 2628/2002 y lo establecido por la AFIP a los efectos de esta política de certificación. La parte pertinente de esa norma es transcripta a continuación, con las modificaciones contenidas en normas complementarias posteriores.

2.1.2.1.- Obligaciones impuestas por el decreto 2628/2002, artículos 35

Una autoridad de Registro es una entidad responsable de las siguientes funciones:

a) La recepción de las solicitudes de emisión de certificados.

b) La validación de la identidad y autenticación de los datos de los titulares de certificados.

c) La validación de otros datos de los titulares de certificados que se presenten ante ella cuya verificación delegue el Certificador Licenciado.

d) La remisión de las solicitudes aprobadas al Certificador Licenciado con la que se encuentre operativamente vinculada.

e) La recepción y validación de las solicitudes de revocación de certificados; y su direccionamiento al Certificador Licenciado con el que se vinculen.

f) La identificación y autenticación de los solicitantes de revocación de certificados.

g) El archivo y la conservación de toda la documentación respaldatoria del proceso de validación de identidad, de acuerdo con los procedimientos establecidos por el certificador licenciado.

h) El cumplimiento de las normas y recaudos establecidos para la protección de datos personales.

i) El cumplimiento de las disposiciones que establezca la Política de Certificación y el Manual de Procedimientos del Certificador Licenciado con el que se encuentre vinculada, en la parte que resulte aplicable.

2.1.2.2.- Obligaciones adicionales y aclaraciones

- La autoridad de Registro es responsable del cumplimiento de las normas y recaudos establecidos para la protección de claves privadas y de seguridad física y lógica.

2.1.3. – Obligaciones de los suscriptores de los certificados

2.1.3.1. - Las obligaciones de los suscriptores de los certificados se originan en la ley 25506, artículo 25:

a) Mantener el control exclusivo de sus datos de creación de firma digital, no compartirlos, e impedir su divulgación;

b) Utilizar un dispositivo de creación de firma digital técnicamente confiable;

c) Solicitar la revocación de su certificado al certificador licenciado ante cualquier circunstancia que pueda haber comprometido la privacidad de sus datos de creación de firma;

d) Informar sin demora al certificador licenciado el cambio de alguno de los datos contenidos en el certificado digital que hubiera sido objeto de verificación.

2.1.3.2.- Obligaciones adicionales y aclaraciones:

- Ingresar con una periodicidad mensual al Portal del suscriptor, para notificarse de los mensajes que pudieran estar presentes en dicho portal.

2.1.4. - Obligaciones de los terceros usuarios

Las obligaciones de los terceros usuarios se originan en la Decisión Administrativa 06/2007 de la JGM y lo establecido por la AFIP a los efectos de esta política de certificación. La parte pertinente de esa norma es transcripta a continuación.

2.1.4.1.- Obligaciones impuestas por la Decisión Administrativa 06/2007 de la JGM, Anexo II:

a) Conocer los alcances de la Política de Certificación conforme los “Términos y condiciones con terceros usuarios”.

b) Rechazar la utilización del certificado para fines distintos a los previstos en la Política de Certificación que lo respalda y de usarlo conforme a los “Términos y condiciones con terceros usuarios”.

c) Verificar la validez del certificado.

2.1.4.2.- Obligaciones adicionales y aclaraciones

- Tomar conocimiento de los términos y condiciones aplicables a los terceros usuarios de los certificados digitales emitidos bajo la presente política, publicados en el sitio web “acn.afip.gov.ar”.

- En caso de que el tercero usuario elija hacer uso del sistema OCSP de consulta del estado de un certificado, también deberá tomar conocimiento del formato del certificado OCSP, y verificar su validez tal como haría con cualquier otro relacionado con la firma digital de un documento que recibe.

2.1.5. - Obligaciones del servicio de repositorio

Las obligaciones del servicio de repositorio se originan en la ley 25506, el decreto 2628/2002, y lo establecido por la AFIP a los efectos de esta política de certificación. La parte pertinente de esas normas es transcripta a continuación, con las modificaciones contenidas en normas complementarias posteriores.

2.1.5.1.- Obligaciones impuestas por la ley 25506, artículo 21, inciso k):

- Publicar en Internet o en la red de acceso público de transmisión o difusión de datos que la sustituya en el futuro, en forma permanente e ininterrumpida, la lista de certificados digitales revocados, las políticas de certificación, la información relevante de los informes de la última auditoría de que hubiera sido objeto, su manual de procedimientos y toda información que determine la autoridad de aplicación.

2.1.5.2.- Obligaciones impuestas por el decreto 2628/2002, artículo 34, incisos g), h) y m):

- Garantizar el acceso permanente, eficiente y gratuito de los titulares y terceros al repositorio de certificados revocados.
- Mantener actualizados los repositorios de certificados revocados por el período establecido por el Ente Administrador.
- Cumplir las normas y recaudos establecidos para la protección de datos personales.

2.1.5.3.- Obligaciones adicionales y aclaraciones

- Disponer y dedicar los recursos necesarios para garantizar la seguridad de los datos almacenados, desde el punto de vista técnico y legal.

2.2. – Responsabilidades

Las responsabilidades se originan en la ley 25506 y lo establecido por la AFIP a los efectos de esta política de certificación. La parte pertinente de esa norma es transcripta a continuación.

> Limitaciones de responsabilidad. Los certificadores licenciados no son responsables en los siguientes casos:
>
> a) Por los casos que se excluyan taxativamente en las condiciones de emisión y utilización de sus certificados y que no estén expresamente previstos en la ley;
>
> b) Por los daños y perjuicios que resulten del uso no autorizado de un certificado digital, si en las correspondientes condiciones de emisión y utilización de sus certificados constan las restricciones de su utilización;
>
> c) Por eventuales inexactitudes en el certificado que resulten de la información facilitada por el titular que, según lo dispuesto en las normas y en los manuales de procedimientos respectivos, deba ser objeto de verificación, siempre que el certificador pueda demostrar que ha tomado todas las medidas razonables.

2.3. – Responsabilidad financiera

2.3.1 Responsabilidad Financiera del Certificador

Las responsabilidades financieras se originan en la ley 25506 y lo establecido por la AFIP a los efectos de esta política de certificación. La parte pertinente de esa norma es transcripta a continuación.

2.3.1.1.- Obligaciones impuestas por la ley 25506, artículo 38

> Responsabilidad de los certificadores licenciados ante terceros.
>
> - El certificador que emita un certificado digital o lo reconozca en los términos del artículo 16 de la presente ley, es responsable por los daños y perjuicios que provoque, por los incumplimientos a las previsio-

nes de ésta, por los errores u omisiones que presenten los certificados digitales que expida, por no revocarlos, en legal tiempo y forma cuando así correspondiere y por las consecuencias imputables a la inobservancia de procedimientos de certificación exigibles. Corresponderá al prestador del servicio demostrar que actuó con la debida diligencia.

2.3.1.2.- Obligaciones adicionales y aclaraciones

La AFIP será responsable por los daños y perjuicios que provoque solo en los siguientes casos:

a) Por los incumplimientos a las previsiones determinadas en la Ley 25.506 y sus reglamentos.

b) Por los errores u omisiones que presenten los certificados digitales que expida o los que reconozca en los términos del art. 16 de la Ley 25.506 de Firma Digital.

c) Por no revocarlos, en legal tiempo y forma cuando así correspondiere.

d) Por las consecuencias imputables a la inobservancia de procedimientos de certificación según la normativa vigente.

2.4. - Interpretación y aplicación de las normas

2.4.1. - Legislación aplicable

La presente Política de Certificación, su correspondiente Manual de Procedimientos y demás documentos asociados, responden a la Ley 25.506, su Decreto reglamentario N° 2628/02, la Decisión Administrativa de la Jefatura de Gabinete de Ministros N° 06/2007 y demás normas aplicables.

La presente Política de Certificación así como su documentación asociada se actualizará al marco normativo que se pudiere dictar en el futuro, comunicándose a través del sitio web “acn.afip.gov.ar”.

2.4.2. - Forma de interpretación y aplicación

La interpretación y/o aplicación de las disposiciones de la presente Política de Certificación y de cualquiera de sus documentos asociados, será resuelta según las normas mencionadas en el punto 2.4.1 y 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 la presente Política de Certificación y/o en cualquiera de sus documentos asociados se ajustará a la Ley 19.549 de Procedimientos Administrativos y 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 no cobrará arancel alguno por los servicios relacionados con esta política de certificación.

La AFIP podrá entregar en forma gratuita dispositivos de hardware móviles para soportar los certificados digitales de Clase 4, y podrá 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

El repositorio de información de la AFIP en su carácter de Certificador Licenciado, se encuentra en el sitio web “acn.afip.gov.ar”.

A través de la dirección de ese sitio web se tendrá acceso a:

- El certificado digital de clave pública de la AC de la AFIP y su estado de validez.
- Información del estado de validez de los certificados emitidos.
- La lista de certificados revocados.
- La presente Política de Certificación y versiones anteriores si las hubiere.
- El Manual de Procedimientos de Certificación correspondiente a la presente Política en sus aspectos públicos, y versiones anteriores si las hubiere.
- El Acuerdo Tipo con Suscriptores correspondiente a la presente Política de Certificación.
- Los Términos y Condiciones con Terceros Usuarios correspondientes a la presente Política de Certificación.
- La Política de Privacidad.
- La información pertinente de los informes de auditorias.
- El repositorio de certificados.
- El certificado OCSP

2.6.2. - Frecuencia de publicación

Las actualizaciones a la información contenida en el repositorio se realizarán en forma inmediata a la disponibilidad de ellas. La publicación de certificados revocados se realizará según lo indicado en el punto específico de esta Política de Certificación.

2.6.3. - Controles de acceso a la información

La AFIP garantiza el acceso permanente, irrestricto y gratuito a la información publicada en su repositorio.

2.6.4. – Repositorios de certificados y listas de revocación

Por medio de su sitio web “acn.afip.gov.ar”, provee información del estado de validez de los certificados emitidos y publica la lista de certificados vigentes revocados correspondientes a la presente Política de Certificación.

2.7. – Auditorías

La AC de la AFIP es susceptible de los procesos de auditoría externa por parte de los Organismos que establezca el Estado Nacional y también por parte de la Autoridad de Aplicación de Firma Digital, dependiente de la Jefatura de Gabinete de Ministros del Poder Ejecutivo Nacional, de acuerdo a lo establecido por el Art. 21 inc. k) y r) y el Art. 33 de la Ley 25.506; y el Art. 20 del Decreto Reglamentario N° 2628/02.

Se publicará en el sitio web “acn.afip.gov.ar” la información pertinente que surja de los informes de las distintas auditorías realizadas. Esa información será mantenida para su consulta hasta que sea reemplazada por la de un nuevo informe del mismo organismo auditor.

Asimismo, la AC de la AFIP es susceptible del proceso de auditoría interna:

- La Unidad de Auditoría Interna de la AFIP es la encargada de efectuar las auditorías.
- Las frecuencias de las auditorías se determinan en virtud de los planes establecidos por dicha Unidad.
- La modalidad de comunicación de los informes de auditoría serán de carácter reservado y dirigido a los responsables de las funciones observadas.

En caso de dictámenes no favorables, el Responsable de la AC de la AFIP implementará las medidas correctivas necesarias.

2.8. – Confidencialidad

2.8.1. - Información confidencial

La información que es recibida por la AFIP en las solicitudes de certificados, será tratada en forma confidencial, dándose a conocer solo los datos que

según el marco normativo así se autoriza, según lo establecido en la Ley de Protección de Datos Personales y aquellos que expresamente consienta el Suscriptor, a excepción de:

a) Un pedido formal de autoridades judiciales.

b) Un pedido formal de otras autoridades con competencia suficiente.

La AFIP obrará con la debida diligencia y cuidado a fin de impedir que los terceros tomen conocimiento de los datos brindados por el Suscriptor.

2.8.2. - Información no confidencial

Se considera información “no confidencial” para la AFIP a:

a) Su propio certificado digital de clave pública y su estado de validez.

b) Información del estado de validez de los certificados emitidos.

c) La lista de certificados revocados.

d) La información incluida en esta Política de Certificación y su correspondiente Manual de Procedimientos.

e) El Acuerdo Tipo con Suscriptores correspondiente a la presente Política de Certificación.

f) La Política de Privacidad de la AC de la AFIP.

g) Los Términos y Condiciones con Terceros Usuarios correspondientes a la presente Política de Certificación.

h) La información pertinente de los informes de las auditorías.

i) Los certificados contenidos en el repositorio.

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

El acceso a las listas de certificados revocados está disponible en forma pública en el sitio web “acn.afip.gov.ar”.

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

2.8.4. – Divulgación de información a autoridades judiciales

Se divulgará la información ante un pedido formal de información emanado de una Autoridad Judicial, sobre cualquiera de los datos o información de un Suscriptor o grupo de ellos.

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

Se divulgará la información ante un pedido formal de información emanado de una Autoridad Administrativa Competente, sobre cualquiera de los datos o información de un Suscriptor o grupo de ellos.

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.

Excepto en los casos previstos en los apartados anteriores, toda divulgación de información referida a los datos de identificación del suscriptor de un certificado digital sólo podrá efectuarse con la previa autorización del suscriptor de ese certificado digital. No será necesario el consentimiento cuando la información haya sido obtenida de fuentes de acceso público irrestrictas.

2.8.7. – Otras circunstancias de divulgación de información

La AFIP podrá proporcionar los datos o información del Suscriptor o grupo de ellos, en todos los casos en que exista una obligación legal de así hacerlo, ajustándose en tal caso a lo que la norma establezca a tales efectos. La AFIP no será responsable por las eventuales consecuencias.

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.

3- IDENTIFICACIÓN Y AUTENTICACIÓN

3.1. - Registro inicial

La AFIP, en su sitio web “acn.afip.gov.ar”, pone a disposición del solicitante de un certificado digital, entre otros documentos, los siguientes:

1) las condiciones de utilización del certificado digital,
2) las características del certificado digital solicitado, entre las cuales se incluirán:
- identificación del suscriptor
- su vigencia
- identificación de la Política de Certificación bajo la cual se emite
- clase de certificado

3) las limitaciones a la responsabilidad,
4) los procedimientos relacionados a las operaciones vinculadas,
5) los efectos de la revocación de su propio certificado digital y de la licencia que le otorga la Autoridad de Aplicación,
6) las obligaciones que el suscriptor asume como usuario del servicio de certificación,

7) los medios a los que el suscriptor puede acudir para solicitar aclaraciones, dar cuenta de mal funcionamiento del sistema, o presentar reclamos.

El proceso de solicitud podrá ser iniciado solamente por el interesado, quien deberá poseer una Clave Fiscal válida y con ella ingresar al sitio web “acn.afip.gov.ar”, solicitando el certificado de la clase que se corresponda con el fin requerido para su utilización. La clase de certificado digital que cada solicitante puede requerir según las exigencias de utilización, puede ser de “Clase 3” (implementado por software) o de “Clase 4” (implementado en un dispositivo de hardware). Luego el solicitante deberá confirmar, rectificar y/o proveer los datos requeridos para la emisión, y seleccionar el Puesto de Atención de la AR donde deberá concurrir dentro de los 30 días corridos, con la documentación que la AC de la AFIP le detallará en la solicitud.

Para ambas clases de certificados, debe ser establecido un Código de Revocación Telefónico por parte del solicitante al momento de confirmar sus datos personales.

La solicitud consta de una serie de pasos que guían al interesado en el proceso. Al finalizar el requerimiento se imprime el formulario de adhesión al “Acuerdo con Suscriptor”.

Al presentarse en el Puesto de Atención de la AR elegido, la aprobación de la solicitud de certificado digital estará sujeta al cumplimiento de los requerimientos para la verificación de la identidad del solicitante y los requisitos específicos en relación a la clase del certificado digital solicitado.

El Responsable del Puesto de Atención de la AR o el Oficial de Registro, que atiende a un solicitante de un certificado digital, podrá denegar o condicionar la aprobación de la solicitud del interesado hasta el efectivo cumplimiento de los requisitos y condiciones establecidos.

Una vez aprobada la solicitud de certificado digital, si es un certificado Clase 3 el solicitante aceptará y podrá instalar el certificado digital en una

instancia posterior, por medio de un código de activación que le provee el Oficial de Registro. Si es un certificado Clase 4, la generación de claves, la aceptación y la instalación del certificado ocurren todas en el Puesto de Atención.

Si un solicitante no concurre dentro de los treinta (30) días de generada su solicitud ante el Puesto de Atención de la AR, dicha solicitud de certificado caducará.

3.1.1. - Tipos de Nombres

Sólo se admitirá el nombre y apellido que figure en la documentación de identificación de la persona. Si al momento de ingresar la solicitud el nombre o apellido mostrado por el sistema no coincidiera con los del documento de identidad, se deberá ingresar los de éste último. Los cambios realizados sólo tendrán efecto en el sistema informático de la AC de la AFIP.

3.1.2.- Necesidad de Nombres Distintivos

El Nombre Distintivo para los certificados Clase 3 y Clase 4 está compuesto por los siguientes campos:

Nombre distintivo del emisor:

a) C=AR
b) ST=Ciudad Autónoma de Buenos Aires
c) O=Administración Federal de Ingresos Públicos.
d) Serial Number= CUIT 33693450239
e) CN=Autoridad Certificante de la AFIP

Nombre distintivo del suscriptor:

f) C=AR
g) O=Administración Federal de Ingresos Públicos
h) OU= Persona física.
i) Serial Number= contiene el tipo y número de CUIT/CUIL/CDI, expresado como texto y respetando el siguiente formato y

codificación: “[tipo]” “[nro]”. Los valores posibles para el campo “tipo” son:

- “CUIT”: Clave Única de Identificación Tributaria.
- “CUIL”: Clave Única de Identificación Laboral.
- “CDI”: Clave de Identificación (para extranjeros).

j) CN= contiene el nombre y apellido que figura en el documento de identidad del suscriptor.

El Nombre Distintivo para el certificado OCSP está compuesto por los siguientes campos:

Nombre distintivo del emisor:

a) C=AR
b) ST=Ciudad Autónoma de Buenos Aires
c) O=Administración Federal de Ingresos Públicos.
d) Serial Number= CUIT 33693450239
e) CN=Autoridad Certificante de la AFIP

Nombre distintivo del suscriptor:

f) C=AR
g) O=Administración Federal de Ingresos Públicos
h) OU= Subdirección General de Sistemas y Telecomunicaciones
i) Serial Number= CUIT 33693450239
j) CN= Servicio OCSP.

3.1.3.- Reglas para la interpretación de nombres

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. El solicitante tiene la posibilidad de corregir sus datos personales desde el Portal de suscriptor, al momento de la solicitud. Si tuviera que realizar una corrección a su CUIL, deberá efectuar lo que se indica en el punto 3.1.5 de la presente Política.

3.1.4. - Unicidad de nombres

La AFIP garantiza que el nombre distintivo indicado en el certificado digital es único para cada solicitante o suscriptor de certificado digital. Para evitar la duplicidad de nombres se utilizará el CUIL/CUIT/CDI del solicitante o suscriptor como parte del nombre distintivo.

La posibilidad de suscribir más de un certificado con el mismo CUIL/CUIT/CDI se permite ya que el número de serie del certificado será diferente.

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 suscriptor deberá solicitar la resolución del inconveniente ante el organismo responsable de la emisión de su CUIL, la Administración Nacional de la Seguridad Social (ANSES). En caso de ser un CUIT/CDI, deberá resolverlo ante una Agencia de la AFIP. El solicitante tiene la opción en el Portal de suscriptor, 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 en su fuente de origen deberá realizarse por la vía que corresponda frente al organismo responsable de los mismos.

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 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, el que un paso posterior recibirá la solicitud de certificado digital 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 de los Puestos de Atención de la AR cumplirá las exigencias del Art. 34 inc. i) del Decreto 2628/02, respecto de abstenerse 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 aplicable, ya que no se otorgarán certificados digitales a personas jurídicas.

3.1.9. - Autenticación de la identidad de personas físicas

A fin de lograr la verificación de la identidad de los solicitantes de los certificados de personas físicas, se exige su presencia física en las oficinas del Puesto de Atención de la AR, con la que se encuentre operativamente vinculado.

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 (en caso 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.

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 solicitante o suscriptor de un certificado digital de la AC de la AFIP 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.

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

En caso de que por cualquier causa resultare necesario cambiar el par de claves de un certificado ya emitido, 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.

4. - CICLO DEL CERTIFICADO: REQUERIMIENTOS OPERATIVOS

4.1. - Solicitud de certificado

4.1.1.- Requisitos para la solicitud de certificados digitales:

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 adhirió.

4.1.2.- Presentación de la solicitud:

El solicitante debe iniciar el trámite de solicitud ingresando al Portal de AC de la AFIP “acn.afip.gov.ar”, ir a la opción “Gestione sus certificados” y generar una “Solicitud de certificado” de acuerdo a la clase de certificado digital que requiera, completando los datos que le solicite el sistema y eligiendo un Puesto de Atención de la AR donde continuar el trámite.

En ese mismo acto debe establecer también el Código de Revocación Telefónico.

La emisión de certificados digitales requiere de verificación presencial de identidad. Se debe cumplir lo establecido en el Anexo II de la Resolución General AFIP Nro. 2239 y sus modificatorias posteriores como se menciona

en el punto 3.1.9 de la presente Política, en lo referente a los niveles 3 y 4 de seguridad, respecto de la presentación de documentos de identidad válidos para acreditar la misma, y adicionalmente la documentación de adhesión al “Acuerdo con Suscriptor”.

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 entregará al suscriptor el código de activación de su certificado, el cual será posteriormente utilizado por el suscriptor para aceptarlo e importarlo a su almacén de certificados.

Una vez admitida la solicitud de Clase 4, el Oficial de Registro verificará el dispositivo criptográfico del solicitante y lo orientará en la generación de las claves, en la aceptación del certificado y en su incorporación al dispositivo criptográfico.

4.1.4.- Generación del par de claves criptográficas del suscriptor:

Las particularidades de la generación del par de claves criptográficas del suscriptor dependen de la Clase de Certificado solicitado.

En el caso de Clase 3, el solicitante, al momento de efectuar su solicitud, debió seleccionar si generaría el pedido por medio del navegador o subiendo un archivo con formato PKCS#10 generado por otra aplicación. Si eligió la opción de utilizar el navegador se generó el par de claves en el mismo y la clave privada quedó bajo control del solicitante, a partir de ese momento, en el navegador que estaba utilizando. Si eligió la opción de subir un archivo con formato PKCS#10 generado por otra aplicación, puede retirar posteriormente el certificado digital desde cualquier navegador soportado, en cualquier estación de trabajo.

En el caso de Clase 4, el solicitante ingresa al Portal de suscriptor desde una estación de trabajo del Puesto de Atención usando su clave fiscal. Luego identifica la solicitud de certificado aprobada, conecta su dispositivo criptográfico a un puerto USB de dicha estación y selecciona la opción de generar el par de claves criptográficas que luego será usada para ese certificado.

En el caso del certificado OCSP, la generación de las claves la realiza la AFIP que actúa como suscriptor, además de emisor del certificado.

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. Finalizado el período de validez del par de claves , el certificado digital 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.

Tanto para el caso de Clase 3 como para Clase 4, el suscriptor debe ingresar al Portal de suscriptor mediante su Clave Fiscal, ingresar al menú de renovación de certificado digital, identificar el certificado a renovar y efectuar la solicitud de renovación.

4.2. - Emisión del certificado

El sistema informático de la AC de la AFIP emitirá el certificado tanto para una solicitud de certificado como para una solicitud de renovación.

El solicitante o suscriptor deberá tomar conocimiento de la efectiva emisión de su certificado digital consultando la opción “Mis Trámites” en el Portal de

suscriptor. También recibirá una comunicación por correo electrónico, si hubiera consignado una dirección en la solicitud.

Los certificados Clase 3 y Clase 4 tendrán una validez de 2 (dos) años desde el momento de su emisión. El certificado OCSP tendrá una validez de 9 (nueve) años.

4.3. - Aceptación del certificado

Para aceptar su certificado digital de Clase 3, el suscriptor deberá ingresar al Portal de suscriptor mediante su Clave Fiscal, seleccionar la opción “Mis Trámites”, aceptando su certificado colocando el código de activación que se le entregó al validar su identidad en el Puesto de Atención de la AR. Si el proceso es exitoso, podrá importar el certificado digital en su equipo, por medio de la opción “Mis Certificados”.
Si el Código de Aceptación no es recordado por el solicitante, podrá requerirlo nuevamente al mismo Oficial de Registro que le aprobó la solicitud.

Para el caso de un certificado de Clase 4, la aceptación se produce en el Puesto de Atención de la AR luego de validar la identidad del solicitante y finalizado el proceso de generación de claves.
Luego de esta aceptación, el certificado digital, sea de Clase 3 o Clase 4, se almacenará en el repositorio público de certificados de la AC de la AFIP. En caso de que el suscriptor no acepte el certificado digital dentro de los treinta (30) días corridos desde su emisión, se procederá a la incorporación al repositorio público y su inmediata revocación.
En ambas Clases de certificado, si los procesos de aceptación no son exitosos el Oficial de Registro instruirá al solicitante sobre las acciones correctivas necesarias, dentro del plazo establecido.

4.4. - Suspensión y Revocación de Certificados

4.4.1. - Causas de revocación

Las causas de revocación de certificados se establecen en la ley 25.506, el decreto 2628/2002, y lo establecido por la AFIP a los efectos de esta política de certificación. La parte pertinente de esas normas es transcripta a continuación, con las modificaciones contenidas en normas complementarias posteriores.

4.4.1.1. Causas de revocación establecidas por la ley 25506, artículo 19, inciso e)

1) A solicitud del titular del certificado digital.

2) Si determinara que un certificado digital fue emitido en base a una información falsa, que en el momento de la emisión hubiera sido objeto de verificación.

3) Si determinara que los procedimientos de emisión y/o verificación han dejado de ser seguros.

4) Por condiciones especiales definidas en su política de certificación.

5) Por resolución judicial o de la autoridad de aplicación.

4.4.1.2. Causas de revocación establecidas por el Decreto 2628/2002, Art. 23

a) A solicitud del titular del certificado digital

b) Si se determina que un certificado digital fue emitido en base a una información falsa que en el momento de la emisión hubiera sido objeto de verificación.

c) Si se determina que los procedimientos de emisión y/o verificación han dejado de ser seguros.

d) Por condiciones especiales definidas en las Políticas de Certificación.

e) Por Resolución Judicial o de la Autoridad de Aplicación debidamente fundada.

f) Por fallecimiento del titular.

g) Por declaración judicial de ausencia con presunción de fallecimiento del titular.

h) Por declaración judicial de incapacidad del titular.

i) Si se determina que la información contenida en el certificado ha dejado de ser válida.

j) Por el cese de la relación de representación respecto de una persona.

4.4.1.3. Obligaciones adicionales y aclaraciones

La AFIP procederá a la revocación de los certificados digitales por ella emitidos en los siguientes casos:
a) Si existiera sospecha de que la clave privada del suscriptor se encuentra comprometida.
b) Si se toma conocimiento del fallecimiento del suscriptor del certificado digital.
c) Por disposición de la AFIP debidamente fundada, como por ejemplo incumplimiento por parte del suscriptor de las obligaciones establecidas por la Ley Nro. 25.506, su reglamentación aprobada por el Decreto N° 2628/02, y las normas complementarias y modificatorias; por esta Política; por el Manual de Procedimientos correspondiente a la presente Política o por cualquier otro acuerdo, regulación o ley aplicable; mediando previamente declaración en tal sentido emanada de autoridad competente.
d) En caso de que el suscriptor no acepte explícitamente el certificado digital dentro del período de 30 días contados a partir de su emisión.
f) Por declaración judicial de ausencia con presunción de fallecimiento del Suscriptor, debidamente comunicada a la AFIP.

4.4.2. - Autorizados a solicitar la revocación.

La AFIP sólo acepta solicitudes de revocación realizadas por:

- el suscriptor del certificado digital o aquellos terceros autorizados para tal fin
- la AC de la AFIP o su Autoridad de Registro
- la Autoridad de Aplicación
- autoridad judicial competente.

Para que un titular de un certificado digital de la AC de la AFIP autorice a un tercero a revocar su certificado, debe realizarlo por medio del Servicio de Delegación del titular del certificado, con su Clave Fiscal.

4.4.3.- Procedimientos para la solicitud de revocación

La revocación puede ser solicitada por el titular del certificado (o terceros autorizados) o determinada por la AFIP como emisor del certificado, mediante alguna de las vías previstas en el punto 3.4 de este documento.

4.4.3.1 Revocación por parte del suscriptor:

a) Mediante su Clave Fiscal: debe ingresar al Portal de suscriptor, iniciar sesión, ir al menú "Mis Certificados", identificar su certificado, y efectuar la acción correspondiente de revocación.
b) Por medio de la Mesa de Ayuda de la AC de la AFIP: comunicando su CUIL/CUIT/CDI y su Código de Revocación Telefónico. Dicho código se estableció al solicitar el primer certificado, en la etapa de confirmación de datos personales, es común a todos los certificados activos del suscriptor y puede ser cambiado a voluntad desde el Portal de suscriptor.
c) Presentación personal en cualquier Puesto de Atención de la AR de la AFIP: validando su identidad con un documento de identidad según lo indicado por el Anexo II de la RG AFIP 2239/2007 y modificatorias.

4.4.3.2 Revocación por parte de un tercero autorizado:

a) Un tercero autorizado puede efectuar una revocación sólo por medio de su propia Clave Fiscal, siendo el único medio autorizado.

4.4.3.3 Revocación por parte de la AFIP:

Los Puestos de Atención, por medio de sus Responsables u Oficiales de Registro, son los encargados de efectuar la revocación de los certificados según las causas detalladas en el punto 4.4.1 de la presente Política. Podrán actuar de oficio o por intermedio del

Responsable de la AR o de la AC según correspondan a cada causa de revocación.

Para las causas de revocación con origen en la propia AFIP, las actuaciones quedarán bajo resguardo del Responsable de la AR.

En caso de revocación por medio de la presentación personal ante un Puesto de Atención o por medio de la Mesa de Ayuda invocando el Código de Revocación Telefónico, en el sistema quedará evidencia del procedimiento realizado por medio de la firma digital del operador en la solicitud de revocación.

Una vez efectuada la revocación, se actualiza el estado del certificado digital en el repositorio, permitiendo así la consulta mediante el servicio OCSP, y será incluido en la próxima lista de certificados revocados (CRL).

La AFIP informará al suscriptor del certificado digital revocado en un plazo inferior a las 24 horas contadas a partir de la efectiva revocación, mediante la indicación correspondiente al estado del certificado en el Portal de suscriptor y por medio de una nota a su casilla de correo electrónico, si ésta hubiera sido informada. Además el certificado revocado integrará la Lista de Certificados Revocados, disponible en el sitio web “acn.afip.gov.ar”, y se reflejará su estado en el repositorio de certificados, que se consulta también desde la opción correspondiente de dicha página.

4.4.4. - Plazo para la solicitud de revocación

Una solicitud de revocación se efectuará cuando se presente alguna de las circunstancias previstas en el apartado 4.4.1 de la presente Política de Certificación.

La solicitud recibida será procesada de inmediato, tal como lo exige la normativa legal.

El plazo máximo entre la recepción de la solicitud y el cambio de la información de estado del certificado digital en los sitios de publicación será

de hasta 24 horas para la lista de certificados revocados, e inmediato para el servicio OCSP y la consulta de estado de un certificado.

Las vías de recepción permanente, sin restricciones de fecha y hora, para solicitudes de revocación son:

1) El Portal de suscriptor, por medio de la Clave Fiscal del titular del certificado,

2) El Portal de suscriptor, por medio de la Clave Fiscal del tercero autorizado por el titular del certificado,

3) La Mesa de Ayuda de la AC de la AFIP, por vía telefónica,

4.4.5. – Causas de suspensión

No aplicable.

4.4.6. – Autorizados a solicitar la suspensión

No aplicable.

4.4.7. – Procedimientos para la solicitud de suspensión

No aplicable.

4.4.8. – Límites del período de suspensión del certificado

No aplicable.

4.4.9. - Frecuencia de emisión de listas de certificados revocados

La AFIP mantiene publicada la lista de certificados revocados en forma permanente, efectuando su actualización dentro de un plazo máximo de 24 horas, aun cuando su contenido no hubiera sufrido modificaciones.

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

Será obligación de los terceros usuarios efectuar la verificación de los documentos que reciban firmados digitalmente mediante certificados digitales emitidos por la AC de la AFIP, como se indica a continuación:

-
- Asegurarse de la autenticidad de la lista de certificados revocados (CRL), mediante la verificación de la firma digital de la AC de la AFIP que la emite y de su período de validez.
- Verificar que el certificado digital correspondiente al documento firmado, no se encuentre incluido en la lista de certificados revocados publicada en el sitio web “acn.afip.gov.ar/crl/afipacn.crl”
- Se advierte que los certificados revocados dejan de estar contenidos en la lista de certificados revocados luego de finalizar su periodo de validez.

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

Por medio de la CRL:

Por medio de la lista de certificados revocados se podrá determinar si un certificado digital está revocado.

La AFIP garantiza el acceso permanente y gratuito a la lista de certificados revocados que se publica en el sitio web “acn.afip.gov.ar/crl/afipacn.crl”.

Por medio del servicio OCSP:

Adicionalmente a la lista de certificados revocados, la AFIP provee un servicio de verificación en línea del estado de los certificados, denominado Online Certificate Status Protocol (OCSP) o Protocolo en Línea del Estado de los Certificados. Este servicio se provee por medio del sitio web “acn.afip.gov.ar/ocsp/”. Las respuestas de este servicio son firmadas con la clave del certificado OCSP.

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

El uso del protocolo OCSP permite, mediante su consulta, determinar el estado de un certificado digital y representa una alternativa al servicio de CRLs, el que también estará disponible. Este servicio se provee por medio del sitio web “acn.afip.gov.ar/ocsp”. Usando este protocolo se consulta, por medio del número de serie de un certificado digital, al repositorio de certificados digitales de la AC de la AFIP, detectando e informando el resultado de la consulta.

El resultado de la consulta estará firmado con la clave del certificado OCSP correspondiente.

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

No aplicable.

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

No aplicable.

4.4.15. - Requisitos específicos para casos de compromiso de claves

Es obligación del suscriptor solicitar de inmediato la revocación de su certificado digital cuando la clave privada, o el medio en que se encuentre almacenada, se encuentren comprometidos o corran riesgo cierto de estarlo.

4.5. - Procedimientos de Auditoria de Seguridad

La AFIP implementa un sistema de archivo en soporte papel e informático de las transacciones, que permite mantener en un entorno seguro toda la información considerada relevante y que pueda ser requerida por entidades de auditoría internas y externas, que esté relacionada con los siguientes grupos de eventos:

a) Administración del ciclo de vida de las claves criptográficas
b) Administración del ciclo de vida de los certificados

c) Administración del ciclo de vida de los dispositivos criptográficos
d) Información relacionada con la solicitud de certificados
e) Eventos de seguridad

En el Libro de Actas de la AC de la AFIP se registran los eventos no informatizados asociados a la operación de la AC desde la Ceremonia de Generación de su par de claves criptográficas, las sucesivas modificaciones y actualizaciones de datos del sistema, así como la revocación del certificado digital de la propia AC y creación de uno nuevo por parte de la Autoridad de Aplicación.

La AR de la AFIP, bajo el esquema descentralizado en Puestos de Atención, tiene a disposición del organismo auditor toda la documentación que reciba o genere como respaldo del proceso de validación de la identidad de los solicitantes y suscriptores de certificados, que se conservará en lugar seguro dentro del ámbito de cada Puesto de Atención de la AR por diez (10) años. En el caso de los certificados de suscriptores, el plazo se contará desde la fecha de vencimiento del certificado digital o de su revocación, lo que suceda en último término.

4.6. - Archivo de registros de eventos

La AFIP resguardará en original y copia todo archivo en soporte papel e informático de las transacciones detalladas en el punto 4.5 de la presente Política, a disposición de las entidades de auditoría interna y externas que correspondan por un plazo de diez (10) años.

El Libro de Actas será resguardado dentro de la caja de seguridad dispuesta en el recinto de la AC de la AFIP.

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

El cambio de las claves criptográficas de la AC de la AFIP, podrá ocurrir por la necesidad de:

a) Sustituir las claves que van a ser retiradas, originado por el vencimiento del certificado de la AC.
b) Modificar la información contenida en el certificado, de importancia tal que obligue a solicitar un nuevo certificado a la Autoridad de Aplicación.
c) Producir el cese de esta política y la tramitación de una nueva licencia.

En todos los casos este cambio de clave implica la emisión de un nuevo certificado por parte de la Autoridad de Aplicación a favor de la AC de la AFIP.

La clave privada que es objeto de cambio continuará siendo utilizada para firmar la lista de certificados revocados correspondiente a la Política bajo la cual fueron emitidos, hasta el plazo de validez del último certificado digital emitido con esa clave privada. En ese momento se revocará el certificado objeto del cambio y se destruirá la clave privada asociada al mismo.

Si la clave privada de la AC de la AFIP está comprometida, la Autoridad de Aplicación revocará su certificado y esa clave ya no podrá ser usada para firmar, ni siquiera CRLs. Los certificados de los suscriptores quedarán sin sustento en una situación equivalente a la de revocados.

4.8. - Plan de contingencia y recuperación ante desastres

La AFIP cuenta con un Plan de Contingencia que permite garantizar el mantenimiento mínimo de la operatoria y la recuperación de los recursos comprometidos dentro de las veinticuatro (24) horas de producida una emergencia.

El Plan de Contingencia comprende el conjunto de procedimientos que debe llevar a cabo su personal ante eventos que impidan la continuidad de sus operaciones. El plan es conocido por todo el personal de la AC de la AFIP, e incluye pruebas periódicas para garantizar su implementación efectiva en caso necesario.

La AFIP dispone controles que aseguran:

- La continuidad de las operaciones en caso de desastre.
- La continuidad de las operaciones en caso de la vulneración de su clave privada.

Para ello la AFIP establece procedimientos para minimizar las interrupciones de sus actividades y para proteger los procesos críticos de los efectos de fallas significativas o desastres. El Plan involucra a todos los recursos físicos, de hardware, software, humanos y de información integrantes de su estructura con el fin de garantizar su adecuado y continuo funcionamiento.

La administración de la continuidad de las operaciones incluirá controles destinados a identificar y reducir riesgos, atenuar las consecuencias de los incidentes perjudiciales y asegurar la reanudación oportuna de las operaciones indispensables.

Los procedimientos se encuentran descriptos detalladamente en el referido Plan de Contingencia.

4.9. – Plan de Cese de Actividades

De acuerdo a lo estipulado en el artículo 22 del la Ley N° 25.506, la licencia conferida a la AFIP por la Autoridad de Aplicación a la presente Política de Certificación, puede ser cancelada por:

a) Decisión de la AFIP comunicada a la Autoridad de Aplicación;
b) Por la disolución del organismo;
c) Por cancelación de su licencia dispuesta por la Autoridad de Aplicación, según Art. 44 de la Ley N° 25.506.

La AFIP cuenta con un Plan de Cese de Actividades donde se describen los requisitos y procedimientos a ser adoptados en caso de finalización de los servicios de certificador.

En caso de que la AFIP cese en sus funciones de certificador licenciado, la Autoridad de Aplicación y todos los suscriptores de certificados por ella emitidos serán notificados de inmediato. Esta decisión será publicada en el Boletín Oficial, en el sitio web “acn.afip.gov.ar”, en otro medio de difusión nacional y mediante correo electrónico a cada suscriptor de los certificados hasta ese momento válidos.

Después del cese de actividades se mantendrán las exigencias de seguridad establecidas en esta Política de Certificación para la custodia de archivos y documentación.

5. - CONTROLES DE SEGURIDAD FÍSICA, FUNCIONALES Y PERSONALES

La AFIP cuenta con adecuados controles de seguridad física, funcionales y personales.

5.1.- Controles de Seguridad Física

5.1.1.- Construcción y ubicación de instalaciones

El centro de cómputos donde se encuentran instalados los activos informáticos que componen la AC de la AFIP está ubicado en un Ambiente de Máxima Seguridad (AMS). Dicho AMS es una construcción hermética contra fuego, gases, agua y campos electromagnéticos. Reúne además la característica para protección de equipamientos electrónicos, centros de datos, y medios de soporte de datos.

5.1.2.- Niveles de acceso físico

Se encuentran implementados cinco niveles de acceso físico para el personal autorizado a ingresar y operar en la AC de la AFIP, y en cada nivel se incrementa la exigencia de autenticación y control. Dichos niveles están supervisados por una combinación de personal de seguridad y cámaras de observación directa y grabación de eventos.

5.1.3.- Energía y aire acondicionado

La energía es provista en condiciones adecuadas para garantizar una operación continua y segura, con sistemas de provisión de energía ininterrumpibles, contando además con aire acondicionado en configuración redundante.

5.1.4.- Exposición al agua

El sistema de monitoreo ambiental del AMS cuenta con sensores de temperatura, humedad ambiente, humo, flujo de aire y fluidos, que permiten la detección temprana de eventos indeseables o riesgosos. Los equipos electrónicos se encuentran alojados en gabinetes protegidos de exposición a elementos líquidos.

5.1.5.- Prevención y protección contra incendios

El AMS cuenta con un sistema de detección y extinción de incendios independiente y automático.

5.1.6.- Medios de almacenamiento

El AMS cuenta con una sala dedicada para el resguardo físico de los medios de almacenamiento, con acceso protegido por sensores biométricos. Asimismo, en la sala donde se ubica el equipamiento dedicado a la emisión y revocación de certificados, se encuentran los armarios de seguridad para el resguardo de los medios de almacenamiento y documentación de importancia.

5.1.7.- Disposición de material de descarte

La AC de la AFIP implementa procedimientos para la eliminación de los archivos de información sensitiva a fin de imposibilitar su recuperación, acceso y/o difusión indebida luego de su eliminación.

5.1.8.- Sitio alternativo.

La AFIP mantiene en existencia capacidades externas de procesamiento fuera del lugar donde reside el Sistema Informático productivo de la AC, a los efectos de prever la disponibilidad de los

recursos necesarios de hardware y software, para que puedan mantenerse los servicios indispensables en caso de contingencia.

5.2. - Controles Funcionales

Las funciones relacionadas con la AC de la AFIP, son llevadas a cabo por personal calificado, el cual las realiza de acuerdo a roles pre-asignados que contemplan una adecuada separación de funciones.

El personal es seleccionado y entrenado de manera de proporcionar un ambiente de operación seguro y confiable, siendo evaluado periódicamente en relación a sus capacidades en relación con la continuación de sus actividades y responsabilidades.

Las operaciones sensitivas requieren de la concurrencia de varias personas con diferentes roles, y la autenticación es de manera segura mediante contraseñas y/o dispositivos de validación externos según la criticidad de la operación.

Los roles establecidos para la operación de la AC son los siguientes:

- Definidor
- Desarrollador de Software
- Homologador
- Responsable de la AC de la AFIP.
- Administrador de Servidores.
- Administrador de HSM (Hardware Security Module).
- Responsable de AR.
- Responsable de Puesto de Atención.
- Oficial de Registro.
- Testigo.
- Responsable de Comunicaciones.

- Responsable de Seguridad.
- Administrador de Partición.
- Mesa de Ayuda.
- Auditor.

5.3. - Controles de Seguridad del Personal

La AFIP como certificador licenciado sigue la política de administración de personal establecida por el organismo.

La AFIP emplea personal que cuenta con adecuados controles referidos a:

a) Antecedentes penales, laborales y de calificaciones por medio del proceso de selección que involucra en primera instancia a la Subdirección General de Recursos Humanos de la AFIP.
b) Entrenamiento y capacitación inicial y permanente en relación a las funciones de los servicios de certificación.
c) Frecuencia adecuada de los procesos de actualización técnica en relación a las funciones de los servicios de certificación, que puedan afectar directa o indirectamente sus operaciones.
d) Aplicación de sanciones y medidas disciplinarias por acciones no autorizadas.
e) La experiencia e idoneidad son evaluadas en el área donde el personal cumple sus funciones específicas relativas a los servicios de certificación.
f) El personal es provisto de una credencial de identificación, verificable por medio de una consulta en la página de Internet de la AFIP denominada “Credencial Virtual” (“www.afip.gov.ar/genericos/credencialVirtual/”). Adicionalmente, cuenta con credenciales de habilitación de acceso y enrolamiento en sensores biométricos según los diferentes niveles de seguridad física a los cuales puede tener acceso.

6. - CONTROLES DE SEGURIDAD TÉCNICA

La AFIP protege sus claves criptográficas y otros parámetros de seguridad críticos y realiza controles técnicos sobre las funciones operativas del

certificador, autoridad de registro, repositorios de certificados, suscriptores de certificados y lista de certificados revocados.

6.1. - Generación e instalación del par de claves criptográficas

6.1.1. - Generación del par de claves criptográficas

6.1.1.1. - Generación del par de claves criptográficas de la AC de la AFIP

La AFIP, luego del otorgamiento de la licencia por parte de la Autoridad de Aplicación para esta política, generará el par de claves criptográficas de la AC de la AFIP mediante el procedimiento de Ceremonia de Generación de Claves Criptográficas en las instalaciones de la propia AC de la AFIP. Esa generación se hará en un dispositivo criptográfico seguro, que cumple con las características definidas según FIPS 140-2 Nivel 3, y con una longitud de 4096 bits con algoritmo RSA con un período de vigencia de diez (10) años.

La AFIP es responsable de su par de claves criptográficas, no revela su clave privada a terceros bajo ninguna circunstancia y la almacena en un medio que garantiza su integridad y confidencialidad, estando en todo momento bajo el exclusivo control de ella, garantizando que es única y que se encuentra protegida contra réplicas fraudulentas.

6.1.1.2. - Generación del par de claves criptográficas de suscriptores

En el caso de generar el par de claves criptográficas para un certificado digital Clase 3 (por software), el solicitante debe seleccionar si desea generar el pedido por medio del navegador o subirlo a un archivo de formato PKCS#10 generado por otra aplicación. Si elige la opción de utilizar el navegador, generará el par de claves criptográficas en el mismo y la clave privada queda bajo su control. Si elige la opción de subir a un archivo de formato PKCS#10, podrá retirar posteriormente el certificado digital desde cualquier navegador soportado, en cualquier estación de trabajo.

En el caso de generar el par de claves criptográficas para un certificado digital Clase 4 (por hardware), el solicitante, en presencia del Oficial de Registro que corrobora que el dispositivo criptográfico utilizado es uno de

los homologados, debe conectar su dispositivo a un puerto USB de la estación de trabajo del Puesto de Atención. A continuación y sin la presencia del Oficial de Registro ingresa con su Clave Fiscal al portal del suscriptor, identifica la solicitud aprobada y pendiente de generación de claves, y selecciona la opción de generar el par de claves criptográficas con lo quedan incorporadas al almacén de claves del dispositivo.

El responsable de la Autoridad de Registro, los responsables de los Puestos de Atención y los Oficiales de Registro son suscriptores de certificados digitales Clase 4 de la AC de la AFIP. La generación y resguardo del par de claves criptográficas para cada uno de ellos se efectuará en su respectivo dispositivo criptográfico FIPS 140 (Versión 1 o 2) Nivel 2.

6.1.1.3. - Generación del par de claves criptográficas del certificado OCSP

La AFIP, luego del otorgamiento de la licencia por parte de la Autoridad de Aplicación para esta política, generará el par de claves criptográficas del certificado OCSP mediante el procedimiento de Ceremonia de Generación de Claves Criptográficas en las instalaciones de la propia AC de la AFIP. Esa generación se hará en un dispositivo criptográfico seguro, que cumple con las características definidas según FIPS 140-2 Nivel 3, y con una longitud de 2048 bits con algoritmo RSA con un período de vigencia de 9 (nueve) años.

6.1.2. - Entrega de la clave privada al suscriptor

La AFIP se abstiene de generar, exigir o por cualquier otro medio tomar conocimiento o acceder a los datos privados de creación de firmas de los suscriptores, de acuerdo a lo establecido por la Ley N° 25.506 art. 21 inc. b) y el Decreto N° 2628/02 art. 34 inc. i).

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

La AC de la AFIP recibe una copia de la clave pública del solicitante de un certificado digital, la cual está contenida en un CSR (Certificate Signing Request) en formato PKCS#10, siendo todas estas operaciones registradas a los fines de auditoría.

La entrega de las claves públicas se efectúa según lo indicado en el punto 6.1.1.2.

6.1.4. - Disponibilidad de la clave pública del certificador

La AFIP publica en su sitio web “acn.afip.gov.ar” el certificado digital OCSP, el certificado digital de la AC de la AFIP y el de la AC Raíz de la República Argentina, siendo estos dos últimos los que constituyen la cadena de certificación.

6.1.5. - Tamaño de las claves criptográficas

La longitud de las claves privadas empleadas por la AC de la AFIP en los procesos de firma de certificados y CRL’s, es de 4096 bits.

El tamaño de las claves privadas empleadas por los agentes de los Puestos de Atención de la AR de la AFIP y por el responsable de ésta pueden ser de 1024 o 2048 bits de longitud.

El tamaño de las claves privadas empleadas por los suscriptores de certificados digitales pueden ser de 1024 o 2048 bits de longitud.

El tamaño de la clave privada empleada en el certificado digital de OCSP es de 2048 bits de longitud.

6.1.6. - Generación de parámetros de claves asimétricas

Los parámetros son:

- algoritmo: RSA
- exponente: 3
- longitud: según se indica en el punto 6.1.5

6.1.7. - Verificación de calidad de los parámetros

La generación de las claves de la AC de la AFIP y del certificado OCSP será realizada utilizando dispositivos criptográficos certificados FIPS 140-2 nivel 3, mientras que la generación de las claves del personal de la AR de la AFIP será realizada utilizando dispositivos criptográficos certificados FIPS 140 (Versión 1 o 2) nivel 2, todos los cuales aseguran la calidad de los parámetros requeridos.

La verificación de la calidad de los parámetros de las claves de los solicitantes será realizada por el sistema informático de la AC de la AFIP, en el momento de recepción de la solicitud de certificado digital. Esa verificación incluye la correcta longitud de las claves y de los parámetros de los certificados digitales, tanto de Clase 3 como de Clase 4.

En caso de ser utilizado un dispositivo criptográfico provisto por el suscriptor, el Oficial de Registro del Puesto de Atención verificará que el mismo se corresponda con alguno de los modelos homologados por la AFIP, mediante los procedimientos establecidos al respecto.

6.1.8. - Generación de claves por hardware o software

El par de claves criptográficas empleado por la AC de la AFIP para la firma de certificados y listas de certificados revocados, y el par de claves criptográficas del certificado OCSP son generadas por medio de dispositivos criptográficos certificados bajo normas FIPS 140-2 Nivel 3.

El par de claves de los responsables de los Puestos de Atención, de los Oficiales de Registro y del Responsable de AR es generado y almacenado en dispositivos criptográficos certificados bajo normas FIPS 140 (Versión 1 o 2) Nivel 2.

El par de claves criptográficas de los certificados digitales de Clase 3 puede ser generado por el solicitante en su navegador o bien mediante algún otro método, también bajo control del solicitante.

El par de claves de los certificados digitales de Clase 4 es generado por el solicitante y almacenado en dispositivos criptográficos certificados bajo

normas FIPS 140 (Versión 1 o 2) Nivel 2 durante el proceso de solicitud del certificado digital, en el Puesto de Atención de la AR.

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

La clave privada de la AC de la AFIP tiene el propósito de ser utilizada para la firma de los certificados de sus suscriptores y para la firma de su Lista de Certificados Revocados (CRL).

La clave privada del certificado OCSP tiene el propósito de ser utilizada para firmar las respuestas del servicio OCSP.

Las claves privadas de los suscriptores de certificados solo podrán ser utilizadas para propósitos de firma digital y no repudio.

6.2. - Protección de la clave privada.

6.2.1. - Estándares para dispositivos criptográficos

El dispositivo criptográfico de generación, almacenamiento y gestión de claves de la AC de la AFIP y del certificado OCSP, cumple con el estándar FIPS 140-2 Nivel 3.

Para el personal de la AR, el estándar correspondiente es FIPS 140 (Versión 1 o 2) Nivel 2.

Para los suscriptores de certificados digitales Clase 4, el estándar correspondiente es FIPS 140 (Versión 1 o 2) Nivel 2.

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

La AC de la AFIP implementa los procedimientos que requieren la participación de testigos para la activación de su clave privada.

La seguridad de este control está garantizada por el uso del dispositivo criptográfico que opera en modo FIPS 140-2 Nivel 3.

6.2.3. - Recuperación de clave privada

Ante una situación que requiera recuperar la clave privada de la AC de la AFIP y que no fuera producto de su compromiso, la AFIP cuenta con procedimientos y elementos para su restauración. Esta tarea es efectuada dentro del recinto de la AC de la AFIP, con personal técnico de la propia AC y los funcionarios testigos que legitiman la operación.

6.2.4. - Copia de seguridad de clave privada

La AFIP mantiene una copia de seguridad de la clave privada de la AC de la AFIP y del certificado OCSP, tanto en el sitio de operaciones principal como en el alternativo, almacenada y protegida de la misma forma e igual plazo que la clave original.

No se mantienen copias de las claves privadas de los suscriptores de certificados digitales.

6.2.5. - Archivo de clave privada

Cuando la clave privada de la AC de la AFIP está desactivada, el dispositivo criptográfico que la contiene permanece bajo el mismo control de seguridad física descripto en el punto 5 de la presente Política de Certificación.

6.2.6. - Incorporación de claves privadas en dispositivos criptográficos

El par de claves criptográficas de la AC de la AFIP y del certificado OCSP se genera y almacena en dispositivos criptográficos conforme lo establecido en la presente política. Sólo se realizan dos transferencias de la clave privada de la AC de la AFIP y del certificado OCSP, correspondientes a sendos backups, uno para el sitio de operaciones principal y el otro para el sitio

alternativo, utilizando los procedimientos de resguardo propios de los dispositivos criptográficos utilizados.

La clave privada de la AC de la AFIP, se crea dentro del dispositivo criptográfico en el momento de la Ceremonia de Generación de Claves Criptográficas. En caso necesario, la incorporación posterior de la misma clave privada al dispositivo criptográfico de la AC de la AFIP, se realiza mediante la restauración del resguardo correspondiente. Ambos eventos son llevados a cabo por medio de procedimientos que involucran a personal técnico, de seguridad y funcionarios testigos que garantizan la seguridad e integridad de la clave creada o restaurada.

En los dispositivos criptográficos de suscriptores de certificados digitales de Clase 4, la clave privada es generada y almacenada por el mismo dispositivo, sin transferirse ni extraerse bajo ninguna circunstancia.

La creación y almacenamiento de la clave privada para los suscriptores de certificados digitales de Clase 4, se realiza cuando el solicitante inserta su dispositivo criptográfico en la estación de trabajo del Puesto de Atención provista a tal fin, seleccionando la opción "Generar clave” para Certificados Clase 4.

6.2.7. - Método de activación de claves privadas

Para la activación de la clave privada de la AC de la AFIP se aplican procedimientos que requieren la participación de los testigos según el control “M de N”, que consiste en la participación de al menos “M” funcionarios de un total de “N” designados, externos a la AC de la AFIP, que validan las operaciones críticas autorizando la ejecución de las mismas por medio de llaves especiales que obran en su poder. Estos procedimientos garantizan que se mantenga el nivel de seguridad de las claves.

6.2.8. - Método de desactivación de claves privadas

La desactivación de claves privadas se lleva adelante mediante el procedimiento de desactivación de partición; cuando se requiere utilizar temporalmente un equipamiento de respaldo o se realicen tareas de mantenimiento. Para efectuarlo se requiere la presencia de personal técnico, de seguridad y de funcionarios testigos que garanticen la operación.

6.2.9. - Método de destrucción de claves privadas

Las claves privadas se destruyen mediante procedimientos que imposibilitan su posterior recuperación o utilización, bajo las mismas medidas de seguridad que se emplearon para su creación.

6.3. - Otros aspectos de administración de claves

6.3.1.- Archivo permanente de la clave pública

Los certificados digitales, con sus claves públicas, se almacenan en el repositorio de certificados digitales, permitiendo de este modo la verificación de su integridad y de su vigencia por medio del servicio asociado en el sitio web de la AC de la AFIP.

Los repositorios de certificados digitales se encuentran en el sitio web “acn.afip.gov.ar”.

6.3.2. - Período de uso de clave pública y privada

La clave privada asociada con el certificado digital de la AC de la AFIP, tiene una validez de diez (10) años, y de no mediar una revocación anticipada, se lo utilizará para firmar certificados de suscriptores hasta 2 (dos) años antes del vencimiento.

La clave privada asociada con el certificado digital OCSP, tiene una validez de nueve (9) años y, de no mediar una revocación anticipada, se lo utilizará para firmar las respuestas del servicio OCSP durante su período de validez.

El certificado digital de suscriptores de la AC de la AFIP tendrá un período de validez de 2 (dos) años contados desde el momento de su emisión. La validez del par de claves criptográficas es coincidente con la validez del respectivo certificado digital y sus renovaciones si las hubiere. A esos efectos puede verse el punto 4.1.5 del presente documento.

6.4. - Datos de activación

6.4.1.- Generación e instalación de datos de activación

Los datos de activación del dispositivo criptográfico de la AC de la AFIP tienen un control “M de N” en base a “M” funcionarios testigos que deben estar presentes de un total de “N” funcionarios posibles. La AFIP cuenta con procedimientos aseguran el correcto uso de los datos de activación.

Las pautas para la generación de datos de activación de las claves privadas de los dispositivos criptográficos de los suscriptores están detalladas en el procedimiento de generación de claves para certificados digitales.

6.4.2. - Protección de los datos de activación

Los datos de activación deben ser tratados como información confidencial y no deben estar expuestos en medios accesibles por terceros. Las personas responsables de su custodia no deben divulgar su condición.

Las pautas para la protección de los datos de activación de las claves criptográficas de los suscriptores, incluyen mantener el control exclusivo de sus datos de creación de firma digital, no compartirlos, impedir su divulgación y aplicar las medidas de seguridad necesarias para evitar que terceros puedan tomar conocimiento de cualquier dato privado relacionado con su certificado digital. Los propios suscriptores serán responsables del cumplimiento de las mismas.

6.4.3. – Otros aspectos referidos a los datos de activación

No aplica.

6.5. - Controles de seguridad informática

6.5.1.- Requisitos Técnicos específicos

La AFIP, para asegurar su política de seguridad informática, cumplimenta los siguientes requisitos:

a) El acceso al Portal de la AC de la AFIP por parte de los solicitantes y suscriptores de certificados, se efectúa empleando el mecanismo de autenticación de Clave Fiscal.
   La lista de los roles afectados a la operación de los servicios de certificación se encuentra en el punto 5.2 de este documento.
b) Los roles de certificación se determinan de manera de garantizar una adecuada segregación de funciones.
c) La autenticación del personal de la AFIP involucrado en la operatoria del sistema informático de la AC de la AFIP, se efectúa por medio de Clave Fiscal, que se implementa por medio de un dispositivo de autenticación externo. La aprobación de solicitudes de emisión, revocación y renovación de certificados es firmada digitalmente por el personal de los Puestos de Atención utilizando el dispositivo criptográfico que aloja su certificado digital de Clase 4.
d) Se utiliza criptografía para las sesiones de comunicación y acceso a las bases de datos.
e) Se almacenan archivos de datos históricos y de auditoria del certificador y de los trámites de los solicitantes y suscriptores de certificados en relación al proceso de certificación.
f) Se registran los eventos de seguridad producidos en el proceso de certificación.
g) Se efectúan pruebas de seguridad periódicas relativas a los servicios de certificación. La AFIP establece procedimientos para la protección y el control de los servicios tanto internos como

externos, garantizando interfaces adecuadas entre la red de la organización y las redes de otras organizaciones, y aplicando mecanismos de autenticación apropiados para usuarios y equipamiento.

h) Para la identificación confiable de los roles afectados al proceso de certificación, el sistema identifica a los usuarios por medio de los servicios de autenticación de Clave Fiscal, atribuyéndole el perfil que le corresponda dentro del sistema informático de la AC de la AFIP.

i) Para la recuperación de claves, restauración de parte o todo el sistema y activación del sistema de respaldo, están disponibles los datos de configuración del sistema y los archivos de respaldo en el sitio alternativo.

6.5.2.- Calificaciones de seguridad computacional

El sistema operativo utilizado en los servidores cuenta con certificación EAL4+.

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

6.6.1. - Controles de desarrollo de sistemas

Por medio de controles llevados a cabo por el personal afectado a tareas de homologación de sistemas informáticos, se controla que el diseño se corresponda con la puesta en producción.

La AFIP utiliza estándares para el desarrollo y mantenimiento de la seguridad de sistemas informáticos basados en el modelo OWASP (Open Web Application Security Project).

6.6.2. – Administración de controles y seguridad

La AFIP mantiene el control de los equipos por medio del inventario y de la documentación de la configuración del sistema, registrándose de inmediato

toda modificación o actualización a cualquiera de ellos. Los controles son auditados en forma periódica según las especificaciones de la Política de Seguridad.

El esquema de seguridad física del recinto de la AC de la AFIP, previene que terceros no autorizados puedan ingresar indebidamente a sus instalaciones.

Un control periódico de integridad del sistema de archivos de la AC y su verificación contra una base de registro de cambios, advierte sobre cualquier cambio realizado, lo identifica y permite comprobar su validez.

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

No aplica.

6.7. - Controles de seguridad de red

La AFIP posee mecanismos de control de acceso basados en una estructura separada de autenticación y de autorización de acceso a los sistemas, por medio del sistema de Clave Fiscal.

La AFIP posee un sistema de protección integral de sus activos informáticos, mediante la implementación de soluciones tipo "firewall" (filtrado de paquetes) y sistemas de detección de intrusiones online.

6.8. - Controles de ingeniería de dispositivos criptográficos

El dispositivo criptográfico utilizado por la AC de la AFIP está certificado por el NIST (National Institute of Standards and Technology - Instituto Nacional de Normas y Tecnología de los Estados Unidos) con FIPS 140-2 Nivel 3.

El dispositivo criptográfico utilizado por los suscriptores de certificados digitales Clase 4, incluidos los integrantes de la Autoridad de Registro y Puestos de Atención de la AC de la AFIP, están certificados por NIST con FIPS 140 (Versión 1 o 2) Nivel 2.

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

7.1. - Perfil del certificado

Todos los certificados correspondientes a la presente Política de Certificación serán emitidos conforme con lo establecido en la especificación ITU X.509 versión 3 y cumplen con la estructura siguiente:

Atributos/Extensiones	Contenido
Versión	2 (correspondiente a versión 3)
Número de serie (serial number)	Número asignado por la AC de la AFIP
Algoritmo de firma (signature algorithm)	sha1WithRSAEncryption
Nombre distintivo del emisor (issuer DN)	C=AR, ST=Ciudad Autónoma de Buenos Aires O=Administración Federal de Ingresos Públicos serialNumber=CUIT 33693450239, CN=Autoridad Certificante de la AFIP
Validez (desde, hasta) (Valid From / Valid To)	Not Before: fecha y hora GMT Not After: fecha y hora GMT
Nombre distintivo del suscriptor (subject DN)	C=AR, O=Administración Federal de Ingresos Públicos, OU=Persona Física serialNumber=CUIL/CUIT/CDI (del suscriptor), CN=Nombre y Apellido del suscriptor
Clave pública del suscriptor (Subject Public Key)	rsaEncryption RSA Public Key: (1024/2048/4096 bit)
Limitaciones básicas	CA: Falso
Uso extendido de clave (extended key usage)	* Autenticación para el Cliente Web por medio del Protocolo de Seguridad de la Capa de Transporte (TLS Web Client Authentication) * Protección de e-mail (e-mail Protection)
Identificador de la clave pública de la autoridad certificante (Authority Key Identifier)	Contiene un hash de 20 bytes del atributo Clave pública del certificado de la AC de la AFIP
Punto de distribución de CRL (CRL Distribution Point)	Sitio: http://acn.afip.gov.ar/crl/afipacn.crl http://acn1.afip.gov.ar/crl/afipacn.crl
Uso de claves (Key Usage)	Los bits deben estar como se indican: DigitalSignature = 1 NonRepudiation =1 KeyEncipherment = 1 DataEncipherment = 0 KeyAgreement = 0 KeyCertSign = 0 CRLSign = 0 EncipherOnly = 0
Identificador de la clave del suscriptor (Subject Key Identifier)	Contiene un hash de 20 bytes del atributo Clave pública del suscriptor
Política de certificación (Certificate Policies)	OID: 2.16.32.1.1.1. Sitio CPS: “http://acn.afip.gov.ar/cps” User notice: Este certificado es emitido por la AC

	de la AFIP, certificador licenciado en el marco de la Ley Argentina Nro. 25.506. Clase de certificado X, donde X corresponde a la clase de certificado (3 o 4).
qcStatements	Contiene el nombre de la autoridad de registro y el OID del tipo de certificado: 1.3.6.1.4.1.24035.1.3.1.1 Certificado Clase 3 1.3.6.1.4.1.24035.1.3.1.2 Certificado Clase 4
Authority Information Access	CA Issuers: URI:http://acn.afip.gov.ar/crt/afipacn.crt OCSP: URI:http://acn.afip.gov.ar/ocsp/
Nombres alternativos del suscriptor (Subject Alternative Name)	Este atributo está presente solo si el suscriptor expresó que deseaba que su e-mail se incorpore en el certificado. En dicho caso, el contenido es la dirección de e-mail declarada por el mismo.
Signature Algorithm	Algoritmo de firma del certificado.

7.2. - Perfil de la lista de certificados revocados

Las listas de certificados revocados correspondientes a la presente Política de Certificación son emitidas conforme con lo establecido en la especificación ITU X.509 versión 2 y cumplen con las siguientes indicaciones:

Atributos/Extensiones	Contenido
Versión (Version)	1 (Corresponde a versión 2)
Algoritmo de firma (signature)	sha1WithRSAEncryption
Nombre distintivo del emisor (issuer)	C=AR, ST=Ciudad Autónoma de Buenos Aires O=Administración Federal de Ingresos Públicos serialNumber=CUIT 33693450239, CN=Autoridad Certificante de la AFIP
Día y hora de vigencia (thisUpdate)	Día y hora de emisión de esta CRL, GMT
Próxima actualización (nextUpdate)	Día y hora de emisión de la próxima CRL, GMT
Identificador de la clave pública de la Autoridad Certificante (AuthorityKeyIdentifier)	Contiene un hash de 20 bytes del atributo Clave pública del certificado del suscriptor
Número de CRL (CRLNumber)	Número que se incrementa cada vez que cambia una CRL.
Certificados revocados (revokedCertificates)	Lista de los certificados revocados incluyendo número de serie, fecha de revocación y motivo de la revocación.
Signature Algorithm	Algoritmo de firma del certificado.

7.3. - Perfil del certificado OCSP

El perfil del certificado OCSP es el siguiente:

Atributos/Extensiones	Contenido
Versión	2 (correspondiente a versión 3)
Número de serie (serial number)	Número asignado por la AC de la AFIP
Algoritmo de firma (signature algorithm)	sha1WithRSAEncryption
Nombre distintivo del emisor (issuer DN)	C=AR, ST=Ciudad Autónoma de Buenos Aires O=Administración Federal de Ingresos Públicos serialNumber=CUIT 33693450239, CN=Autoridad Certificante de la AFIP
Validez (desde, hasta) (Valid From / Valid To)	Not Before: fecha y hora GMT Not After: fecha y hora GMT
Nombre distintivo del suscriptor (subject DN)	C=AR, O=Administración Federal de Ingresos Públicos, OU=Subdirección General de Sistemas y Telecomunicaciones serialNumber=CUIT 33693450239, CN=Servicio OCSP
Clave pública del suscriptor (Subject Public Key)	rsaEncryption RSA Public Key: (1024/2048/4096 bit)
Limitaciones básicas	CA: Falso
Uso extendido de clave (extended key usage)	OCSP Signing
Identificador de la clave pública de la autoridad certificante (Authority Key Identifier)	Contiene un hash de 20 bytes del atributo Clave pública del certificado de la AC de la AFIP
Punto de distribución de CRL (CRL Distribution Point)	Sitio: “http://acn.afip.gov.ar/crl/afipacn.crl”
Uso de claves (Key Usage)	Los bits deben estar como se indican: DigitalSignature = 1 NonRepudiation =1 KeyEncipherment = 0 DataEncipherment = 0 KeyAgreement = 0 KeyCertSign = 0 CRLSign = 0 EncipherOnly = 0
Identificador de la clave del suscriptor (Subject Key Identifier)	Contiene un hash de 20 bytes del atributo Clave pública del suscriptor
Política de certificación (Certificate Policies)	OID: 2.16.32.1.1.1 Sitio CPS: “http://acn.afip.gov.ar/cps” User notice: Este certificado es emitido por la AC de la AFIP, certificador licenciado en el marco de la Ley Argentina Nro. 25.506. Clase de certificado OCSP.
qcStatements	Contiene el nombre de la autoridad de registro y el OID del tipo de certificado: 1.3.6.1.4.1.24035.1.3.1.3 Certificado OCSP
Authority Information Access	CA Issuers: URI:http://acn.afip.gov.ar/crt/afipacn.crt OCSP: URI:http://acn.afip.gov.ar/ocsp/
Signature Algorithm	Algoritmo de firma del certificado.

8. - ADMINISTRACIÓN DE ESPECIFICACIONES

8.1. - Procedimientos de cambio de especificaciones

La AFIP, en su carácter de certificador licenciado, cuenta con procedimientos de administración de cambios para efectuar cualquier modificación a la presente Política de Certificación. Toda modificación será sometida a la aprobación de la Autoridad de Aplicación.

8.2. - Procedimientos de publicación y notificación

La AFIP, en su carácter de certificador licenciado, informará a los suscriptores de certificados acerca de todos aquellos cambios que se efectúen a esta Política de Certificación, luego de obtener la aprobación de la validez de los nuevos documentos por parte de la Autoridad de Aplicación, o en todos los casos que la norma así lo imponga.

Las nuevas versiones, que incluirán las modificaciones indicadas, son publicadas en el sitio web “acn.afip.gov.ar”, disponible sin restricción alguna y de acuerdo a lo establecido en el marco normativo.

8.3. - Procedimientos de aprobación

Se establece que la presente Política de Certificación de la AFIP está sometida a aprobación de la Autoridad de Aplicación durante el proceso de licenciamiento, lo mismo que cualquier modificación posterior que se realice a la misma, según lo estipula la Ley N° 25.506 art. 21 inc. q) y reglamentaciones complementarias.

9. - GLOSARIO

Algoritmo RSA: algoritmo utilizado para codificar información que utiliza una clave pública que se debe distribuir en forma segura, y otra privada, la cual es guardada en secreto por su propietario. La seguridad de este algoritmo radica en que no hay maneras rápidas conocidas para conocer la codificación empleada.

Autoridad de Aplicación: la Secretaría de Gabinete y Gestión Pública (SGP) de la Jefatura de Gabinete de Ministros es la Autoridad de Aplicación de firma digital en la República Argentina.

Autoridad de Registro: es la entidad que tiene a su cargo las funciones de validación de la identidad y otros datos de los solicitantes de certificados digitales. Dichas funciones son delegadas por el certificador licenciado.

Certificado Digital: se entiende por certificado digital al documento informático firmado electrónicamente por un certificador, que vincula los datos de verificación de firma a su titular (artículo 13, Ley N° 25.506).

Certificado OCSP: Es un certificado digital emitido por la AC de la AFIP, para ser usado por la AC de la AFIP en la firma de las respuestas a las consultas realizadas mediante el servicio OCSP.

Certificador Licenciado: se entiende por certificador licenciado a toda persona de existencia ideal, registro público de contratos u Organismo Público que expide certificados, presta otros servicios en relación con la firma digital y cuenta con una licencia para ello, otorgada por la Autoridad de Aplicación.

Clave Fiscal: es el método de autenticación de una persona física por medio de sistemas informáticos, a los fines de su individualización segura, y a los efectos de realizar sus trámites o gestiones ante la AFIP.

Código de Activación de Certificado: es un número provisto por el sistema informático de la AC y entregado al solicitante de un certificado, para que por medio del mismo efectúe la acción de aceptación de su certificado. Es único y válido sólo para un determinado certificado emitido.

Código de Revocación Telefónico: es un conjunto de al menos 4 letras y 2 números en cualquier orden, definido por el usuario, que le permitirá revocar un certificado de su propiedad, contactando a la Mesa de Ayuda de la AC de la AFIP. Es único y válido para revocar cualquier certificado que se encuentre vigente.

Control “M de N”: sistema de confianza y garantía para la ejecución de tareas o comandos críticos dentro de un sistema informático, que exige la concurrencia mínima de “M” entidades distintas (personas) de un total designado de “N”, para poder ejecutar dicha tarea o comando. “N” se elige mayor que “M” para garantizar la disponibilidad adecuada de este sistema de confianza.

CUIL/CUIT/CDI: Código Único de Identificación Laboral / Código Único de Identificación Tributaria / Código de Identificación. Identificador compuesto por 11 (once) caracteres numéricos que identifican a un contribuyente, y que es único.

Dispositivos FIPS 140: dispositivos criptográficos que cumplen con el estándar de la Federal Information Processing Standards, en cuanto al cumplimiento de parámetros de seguridad para el resguardo de claves y contenidos digitales.

Firma digital: se entiende por firma digital al resultado de aplicar a un documento digital un procedimiento matemático que requiere información de exclusivo conocimiento del firmante, encontrándose ésta bajo su absoluto control. La firma digital debe ser susceptible de verificación por terceros usuarios, tal que dicha verificación simultáneamente permita identificar al firmante y detectar cualquier alteración del documento digital, posterior a su firma.

Libro de Actas: documento foliado en el que se registran todos los eventos cuyo suceso no esté contemplado en el Sistema Informático de la AC de la AFIP por medio de procedimientos de registro digital que ofrezcan igual o mayor nivel de seguridad. La información mínima a registrar es la siguiente: fecha y hora, personal involucrado, detalle del evento, identificación del funcionario autorizado de la AC de la AFIP que efectúa el registro y de los restantes involucrados que hubiere.

Lista de certificados revocados (CRL): lista de certificados que han sido dejados sin efecto en forma permanente por el certificador licenciado, la cual ha sido firmada digitalmente y publicada por el mismo.

Manual de Procedimientos de Certificación: conjunto de prácticas utilizadas por el certificador licenciado para la administración de certificados digitales.

Modelo OWASP: conjunto de estándares (Open Web Application Security Project) para el desarrollo y mantenimiento de la seguridad en sistemas informáticos.

Plan de Seguridad: conjunto de políticas, prácticas y procedimientos destinados a la protección de los recursos del certificador licenciado.

Plan de Cese de Actividades: conjunto de actividades a desarrollar por el certificador licenciado en caso de finalizar la prestación de sus servicios de certificación.

Plan de Contingencia: conjunto de procedimientos a seguir por el certificador licenciado ante situaciones que comprometan la continuidad de sus operaciones.

Política de Certificación: conjunto de criterios que indican la aplicabilidad de un certificado a un grupo de usuarios en particular.

Política de Privacidad: conjunto de declaraciones que el Certificador Licenciado se compromete a cumplir, de manera de resguardar los datos de los solicitantes y suscriptores de certificados digitales por él emitidos.

Portal de la AC de la AFIP: página correspondiente al sistema informático de la AC de la AFIP donde se accede de forma irrestricta y sin necesidad de autenticación alguna.

Portal de suscriptor: página correspondiente al sistema informático de la AC de la AFIP, desde donde ingresan el solicitante o suscriptor de un

certificado digital por medio de su Clave Fiscal o sus terceros autorizados por medio del Servicio de Delegación.

Puesto de Atención de la AR: lugar adecuadamente preparado donde el Oficial de Registro atiende personalmente al solicitante o suscriptor de un certificado digital para su identificación y autenticación. En él también se reciben consultas o peticiones y se resguarda la documentación relacionada con solicitantes y suscriptores de certificados digitales.

Protocolo PKCS#10: es un formato electrónico estandarizado para realizar requerimientos de certificados digitales.

Servicio de Delegación: es un servicio de Clave Fiscal que permite, por parte de un titular, designar a un representante que podrá actuar en su nombre, en aquellas gestiones habilitadas para efectuarse por medio de este servicio.

Servicio OCSP: servicio de verificación en línea del estado de los certificados (Online Certificate Status Protocol). El OCSP es un método para determinar el estado de revocación de un certificado digital usando otros medios que no sean el uso de Listas de Revocación de Certificados (CRL). El resultado de una consulta a este servicio está firmado por la clave de un certificado de la autoridad que lo brinda, referenciado como “Certificado OCSP” en este documento.

Solicitante: todo potencial suscriptor de un certificado digital provisto por la AC de la AFIP, bajo el marco enunciado en los puntos 1.3.3.- “Suscriptores de Certificados” y 1.3.4.- “Aplicabilidad” de la presente Política de Certificación.

Suscriptor: persona física a cuyo nombre se emite un certificado y posee una clave privada que se corresponde con la clave pública contenida en el mismo.

Terceros usuarios: persona física o jurídica que recibe un documento firmado digitalmente y que genera una consulta para verificar la validez del certificado digital correspondiente (artículo 3, Decreto N° 724).