87

Jefatura de Gabinete de Ministros
Secretaría de Gabinete y Gestión Pública

ES COPIA
ESTELA PLON
Jefa Dpto. Trámites y Protocolizaciones
Jefatura de Gabinete de Ministros

BUENOS AIRES, 17 DIC 2008

VISTO la Ley Nº 25.506, los Decretos Nº 2.628 del 19 de diciembre de 2002 y Nº 1.266 del 31 de julio de 2008, la Decisión Administrativa Nº 6 del 7 de febrero de 2007, la Resolución Nº 63 del 13 de noviembre de 2007 de la ex SUBSECRETARÍA DE LA GESTIÓN PÚBLICA y el Expediente Nº 000235/2008 del registro de la JEFATURA DE GABINETE DE MINISTROS, y

CONSIDERANDO:

Que la Ley Nº 25.506 de Firma Digital reconoce la eficacia jurídica del documento electrónico, la firma electrónica y la firma digital, estableciendo las características de la Infraestructura de Firma Digital de la República Argentina.

J.G.M.
PRODESPA Nº
3303

Que el inciso h) del artículo 30 de la mencionada Ley asigna a la Autoridad de Aplicación la función de otorgar o revocar las licencias a los certificadores y supervisar su actividad, según las exigencias instituidas por la reglamentación.

Que el artículo 24 del Decreto Nº 2.628/02, reglamentario de la Ley Nº 25.506, establece el procedimiento que los certificadores deben observar para la obtención de una licencia y la obligación de presentar la documentación que acredite el cumplimiento de las condiciones estipuladas en la Ley Nº 25.506, su decreto reglamentario y normas complementarias.

Que la Decisión Administrativa Nº 6/07 establece las normas técnicas complementarias del marco normativo de firma digital, aplicables al otorgamiento y revocación de licencias a los certificadores que así lo soliciten, y dispone en su artículo

87

12 que la documentación exigida durante el proceso de licenciamiento conforme lo determinado en su Anexo I "Requisitos para el licenciamiento de certificadores", será considerada confidencial.

Que el citado artículo 12 establece la obligación del ente licenciante de resguardar la información confidencial obrante en las actuaciones de licenciamiento, disponiendo que el ente licenciante sólo procederá a su utilización a los fines de evaluar la aptitud del certificador para cumplir con sus funciones y obligaciones, inherentes al licenciamiento, absteniéndose de proceder a revelarla, utilizarla para otros fines o bien divulgarla a terceros aún después de haber finalizado el proceso de licenciamiento, salvo respecto de aquella información que la normativa vigente establezca como pública.

Que conforme lo previsto en artículo 38 del Decreto Nº 1.759/72, Reglamentario de la Ley Nacional de Procedimiento Administrativo, el carácter reservado o secreto de la documentación contenida en una actuación debe ser declarado tal por decisión fundada y con intervención previa del servicio jurídico.

Que, en consecuencia, y no obstante el carácter confidencial establecido en la normativa reglamentaria, deviene necesario declarar la reserva de la documentación considerada no pública obrante en el Expediente citado en el Visto, dado que la misma contiene información crítica relacionada al funcionamiento y continuidad de las operaciones de la Autoridad Certificante de la ADMINISTRACIÓN DE NACIONAL DE LA SEGURIDAD SOCIAL.

Que la Resolución SSGP Nº 63/07 que aprueba la "Política de Certificación de la Autoridad Certificante Raíz de la Infraestructura de Firma Digital de la República

Argentina", rige la emisión de certificados a los certificadores que hayan sido licenciados por la Autoridad de Aplicación y reconoce a la OFICINA NACIONAL DE TECNOLOGÍAS DE INFORMACIÓN la facultad de asignar el número de identificador de objeto – OID – a la política de certificación licenciada, de acuerdo a lo previsto en el inciso 1.2 de la Introducción del Anexo de la mencionada Resolución.

Que el Decreto Nº 1.266/08 faculta a la SECRETARÍA DE GABINETE Y GESTIÓN PÚBLICA para actuar como Autoridad de Aplicación del Régimen Normativo que establece la Infraestructura de Firma Digital contemplada en la Ley Nº 25.506, como así también, en las funciones de ente licenciante de certificadores, supervisando su accionar.

Que se ha cumplido con todos los recaudos procedimentales establecidos en la normativa, según consta en el Expediente citado en el Visto, a saber: a fs. 1/9 obra la nota de la ADMINISTRACIÓN NACIONAL DE LA SEGURIDAD SOCIAL, por la cual solicita el licenciamiento de la Política de Certificación; a fs. 821/833 luce el Informe de Auditoría; a fs. 838/842 y a fs. 844 y ss. obran las respuestas de ANSES dando cuenta de las modificaciones producidas en virtud de las observaciones formuladas en el Informe de Auditoría; a fs. 846 y ss. se adjunta la versión final de la Política de Certificación la cual se ajusta a la normativa vigente, a fs. 1345 obra el "Informe de Revisión de documentación", el que analiza el cumplimiento por parte de la ANSES de las observaciones contenidas en el Informe de Auditoría, y a fs. 1349/1358 luce el dictamen legal y técnico correspondiente.

Que en virtud de las constancias del expediente, se han acreditado las condiciones requeridas en la normativa vigente para el licenciamiento de la "Política de

Jefatura de Gabinete de Ministros
Secretaría de Gabinete y Gestión Pública

ES COPIA
ESTER LEON
Jefa Dpto. Familias y Protocolizaciones
Jefatura de Gabinete de Ministros

Certificación para Personas Físicas de la Autoridad Certificante de la ADMINISTRACIÓN NACIONAL DE LA SEGURIDAD SOCIAL - ANSES".

Que la OFICINA NACIONAL DE TECNOLOGÍAS DE INFORMACIÓN y la SUBSECRETARÍA DE TECNOLOGÍAS DE GESTIÓN han tomado la intervención que les compete.

Que ha tomado intervención la DIRECCIÓN GENERAL DE ASUNTOS JURÍDICOS de la SUBSECRETARÍA DE COORDINACIÓN de la JEFATURA DE GABINETE DE MINISTROS.

Que la presente medida se dicta en virtud de las facultades conferidas por la Ley Nº 25.506 y los Decretos Nº 1.759/72 y Nº 1.266/08.

J.G.M. PRODESPA Nº 3303 F.

Por ello,

EL SECRETARIO DE GABINETE Y GESTIÓN PÚBLICA
DE LA JEFATURA DE GABINETE DE MINISTROS
RESUELVE:

ARTÍCULO 1°.- Apruébase la "Política de Certificación para Personas Físicas de la Autoridad Certificante de la ADMINISTRACIÓN NACIONAL DE LA SEGURIDAD SOCIAL - ANSES", que como ANEXO forma parte de la presente, con ajuste de las prescripciones de la Ley Nº 25.506 de "Firma Digital" y normas complementarias.

ARTÍCULO 2°.- Otórgase la Licencia para operar como Certificador Licenciado a la ADMINISTRACIÓN NACIONAL DE LA SEGURIDAD SOCIAL y ordénase su inscripción en el Registro de Certificadores Licenciados.

ARTÍCULO 3°.- Instrúyese a la OFICINA NACIONAL DE TECNOLOGÍAS DE

ES COPIA
ESTELA LEON
Jefa Dpto. Normas y Protocolizaciones
Jefatura de Gabinete de Ministros

INFORMACIÓN, conforme la Resolución SSGP Nº 63/07, para que proceda en el término de VEINTICUATRO (24) horas a asignar el Identificador de Objeto (OID) correspondiente a la Política de Certificación que se aprueba en la presente Resolución.

ARTÍCULO 4°.- Instrúyese a la Autoridad Certificante Raíz de la República Argentina para que emita el certificado digital correspondiente a la Política de Certificación aprobada por el Artículo 1°.

ARTÍCULO 5°.- Difúndase la presente y su ANEXO, con el número de OID incorporado, en el sitio de Internet de la SECRETARÍA DE GABINETE Y GESTIÓN PUBLICA http://acraiz.gov.ar/cps/cps.ANSES.1.pdf.

ARTÍCULO 6°.- Establécese la reserva de la siguiente documentación del Expediente citado en el Visto:

J.G.M.
PRODESPA Nº
3303
7
881

1. Manual de Procedimientos de Certificación (fs. 63/99);
2. Servicio de Housing – Sitio de Contingencias para Firma Digital de Anses Especificaciones (fs. 156/180);
3. Plan de Cese de Actividades (fs. 181/185);
4. Política de Seguridad de la Autoridad Certificante (fs. 186/200);
5. Procedimientos de Seguridad (fs. 201/221);
6. Evaluación de Riesgos (fs. 222/237);
7. Plan de Contingencias (fs. 240/247);
8. Plataforma Tecnológica (fs. 248/268);
9. Roles y Funciones (fs. 269/276);
10. CD. Anexo (fs. 387);
11. Estándar de Arquitectura de Integración para el Desarrollo de Aplicaciones (fs. 398/407);
12. Pautas para la Autoridad de Registro (fs. 508/517);
13. Política de Seguridad de la Autoridad Certificante (fs. 518/538);
14. Evaluación de Riesgos (fs. 539/579);
15. Plan de Cese de Actividades (fs. 580/593);
16. Plan de Contingencias (fs. 594/604);
17. Manual de Procedimientos de Certificación (fs. 605/652);
18. Roles y Funciones (fs. 653/665);

COORDINACIÓN MESA de ENTRADAS DESPACHO - J.G.M. FOLIO 1418

Jefatura de Gabinete de Ministros
Secretaría de Gabinete y Gestión Pública

ES COPIA
ESTHER PEON
Jefa Dpto. Trámites y Protocolizaciones
Jefatura de Gabinete de Ministros

19. Procedimiento de Contingencia (fs. 666/688);
20. Manual de Procedimientos de Seguridad (fs. 689/797);
21. Plataforma Tecnológica (fs. 798/819);
22. Pautas para la Autoridad de Registro (fs. 908/918);
23. Política de Seguridad de la Autoridad Certificante (fs. 919/938);
24. Evaluación de Riesgos (fs. 950/990);
25. Plan de Cese de Actividades (fs. 991/1004);
26. Plan de Contingencias (fs. 1005/1015);
27. Manual de Procedimientos de Certificación (fs. 1016/1064);
28. Roles y Funciones (fs. 1065/1074);
29. Procedimiento de Contingencias (fs. 1075/1104);
30. Manual de Procedimientos de Seguridad (fs. 1105/1235);
31. Plataforma Tecnológica (fs. 1236/1257).

ARTÍCULO 7°.- Comuníquese, publíquese, dése a la Dirección Nacional del Registro Oficial y archívese.

RESOLUCIÓN SGGP N° 87

J.G.M.
PROCESFA N°
3303

Dr. Juan Manuel Abal Medina
Secretario de Gabinete y Gestión Pública
Jefatura de Gabinete de Ministros

Jefatura de Gabinete de Ministros
Secretaría de Gabinete y Gestión Pública

ES COPIA
ESTELA PERON
Jefa Dpto. Trámites y Protocolizaciones
Jefatura de Gabinete de Ministros

ANEXO – RESOLUCIÓN SGGP Nº 87

Infraestructura de Firma Digital de la República Argentina

Ley 25.506

Política de Certificación para Personas Físicas de la ANSES

1. - INTRODUCCIÓN

1.1. - Descripción general

El presente documento define la Política de Certificación que rige la relación entre la ADMINISTRACIÓN NACIONAL DE LA SEGURIDAD SOCIAL, los suscriptores de certificados digitales emitidos en el ámbito de la presente política y los terceros usuarios que reciban información firmada digitalmente, de conformidad con la Ley N° 25.506, su Decreto Reglamentario N° 2628/2002 y la Decisión Administrativa 6/2007 de la JGM. La licencia es otorgada mediante Resolución N° 87 /2008 de la Secretaría de Gabinete y Gestión Pública. Asimismo, en esta Política se establecen las responsabilidades de:

- la ANSES como Certificador Licenciado,
- la Autoridad de Registro relacionada,
- los solicitantes y suscriptores de certificados digitales, y
- los terceros usuarios receptores de documentos firmados bajo la presente política.

Con respecto a su alcance, esta Política de Certificación para Personas Físicas de la ANSES comprende la emisión de certificados digitales para el personal que preste servicios a ANSES; autorizando el uso de los certificados emitidos para verificar firmas digitales en comunicaciones internas o externas de esta ADMINISTRACIÓN NACIONAL, en sus procedimientos administrativos.

Bajo esta Política de Certificación, la Autoridad de Registro estará bajo la competencia de las áreas con responsabilidad primaria en la administración y gestión de los recursos humanos.

J.G.M. PROTESPA N° 3303

1.2. - Identificación

Nombre: Política de Certificación para Personas Físicas de la ANSES

Versión: 1

Fecha: 17 DIC 2008

URL: https://servicioswww.anses.gov.ar/firmadigital/politica/

OID: <a asignar por la ONTI> OID asignado: 2.16.32.1.1.2

Lugar: Buenos Aires, Argentina

1.3. - Participantes y aplicabilidad

1.3.1. - Certificador

ANSES en su calidad de Certificador Licenciado, con licencia otorgada por *Resolución N° 87 /2008 de la Secretaría de Gabinete y Gestión Pública* como Autoridad de Aplicación, desarrolla las tareas de emisión de certificados digitales según lo establecido por la Ley 25.506 y sus normas complementarias.

1.3.2. - Autoridad de Registro

Las tareas relacionadas con la identificación y autenticación de los solicitantes y suscriptores, la verificación y guarda de la documentación probatoria son realizadas por la Autoridad de Registro.

En el marco de la presente política la función de Autoridad de Registro estará bajo la competencia de las áreas con responsabilidad primaria en la administración y gestión de los recursos humanos.

Para ver cualquier información al respecto ingresar al sitio:

https://servicioswww.anses.gov.ar/firmadigital/

1.3.3. - Suscriptores de certificados

Podrán ser suscriptores de certificados digitales en el marco de la presente política de certificación, aquellas personas físicas que desempeñan funciones para la ANSES con independencia del tipo de relación pudiendo ser funcionarios, empleados, adscriptos, personal designado desde otros organismos, pasantes o contratados de cualquier naturaleza.

1.3.4. - Aplicabilidad

J.G.M.
PRODESPA N°
3303
Fs.

Los certificados emitidos en el marco de la presente Política de Certificación podrán ser utilizados únicamente en:

a) Comunicaciones internas de la ANSES, a través del correo electrónico institucional.

b) Comunicaciones de la ANSES con otros organismos nacionales o internacionales, tanto privados como públicos a través del correo electrónico institucional.

c) Firma de actos administrativos y documentación de incumbencia de esta Administración Nacional, a saber: Resoluciones, Disposiciones, Notas, Circulares, Informes, Memorándum, Dictámenes, Formularios, Parte Diarios y Expedientes, debidamente autorizados.

d) Firma de Convenios y Acuerdos con otras instituciones.

1.4. - Contactos

Esta Política de Certificación es administrada por:

- Gerencia de Sistemas y Telecomunicaciones, ANSES representada por su Gerente a cargo.
- Domicilio: Piedras 353, (C1070AAG) Ciudad Autónoma de Buenos Aires, Argentina
- E-mail: firmadigital@anses.gov.ar
- Teléfono: (011) 4015-2201

Para realizar preguntas, efectuar reclamos o enviar sugerencias referidos al proceso de certificación el interesado deberá dirigirse a:

- Mesa de Ayuda de la Gerencia de Sistemas y Telecomunicaciones de ANSES representada por el Coordinador a cargo
- Domicilio: Piedras 353, (C1070AAG) Ciudad Autónoma de Buenos Aires, Argentina

- E-mail: mesadeayuda@anses.gov.ar
- Teléfono: (011) 4015-2100

2.- ASPECTOS GENERALES DE LA POLÍTICA DE CERTIFICACION

2.1. -Obligaciones

2.1.1. - Obligaciones del certificador

Son obligaciones de ANSES en su carácter de Certificador Licenciado, cumplir con:

a) Las previsiones establecidas en el artículo 21 de la Ley 25.506

- 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, sus características, efectos y responsabilidades, 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 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;
- 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;
- Mantener el control exclusivo de sus propios datos de creación de firma digital e impedir su divulgación;
- Operar utilizando un sistema técnicamente confiable de acuerdo con lo que determine la Autoridad de Aplicación;
- Notificar al solicitante las medidas que está obligado a adoptar para crear firmas digitales seguras y para su verificación confiable, y las obligaciones que asumirá por el solo hecho de ser titular de un certificado;
- Recabar únicamente aquellos datos personales del titular del certificado que sean necesarios para su emisión, quedando el solicitante en libertad de proveer información adicional;
- Mantener la confidencialidad de toda información que no figure en el certificado;
- Poner a disposición del solicitante de un certificado toda la información relativa a su tramitación;
- Mantener la documentación de respaldo de los certificados digitales emitidos, por diez (10) años a partir de su fecha de vencimiento o revocación;
- Incorporar en su política de certificación los efectos de la revocación de su propio certificado y/o de la licencia que le otorgara la Autoridad de Aplicación;
- 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

J.G.M. PRODESPA Nº 3303

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;

- Publicar en el Boletín Oficial aquellos datos que la Autoridad de Aplicación determine;
- Registrar las presentaciones que le sean formuladas, así como el trámite conferido a cada una de ellas;
- Informar en las políticas de certificación si los certificados digitales por él emitidos requieren la verificación de la identidad del titular;
- 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;
- Solicitar inmediatamente a 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;
- Informar inmediatamente a la Autoridad de Aplicación sobre cualquier cambio en los datos relativos a su licencia;
- Permitir el ingreso de los funcionarios autorizados de la Autoridad de Aplicación y de los auditores a su local operativo, poner a su disposición toda la información necesaria y proveer la asistencia del caso;
- 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;
- 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;
- Constituir domicilio legal en la República Argentina;
- Disponer de recursos humanos y tecnológicos suficientes para operar de acuerdo a las exigencias establecidas en la presente ley y su reglamentación;
- Cumplir con toda otra obligación emergente de su calidad de titular de la licencia adjudicada por la Autoridad de Aplicación.

b) Las previsiones establecidas en los artículos 34 y 36 del Decreto N° 2628/02

- 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, según la Política de Certificación bajo la cual se solicita.
- Mantener a disposición permanente del público las Políticas de Certificación y el Manual de Procedimientos correspondiente.

J.G.M. PRODESPA N° 3303 7

- Cumplir cabalmente con las políticas de certificación acordadas con el titular y con su Manual de Procedimientos.
- 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.
- Informar al solicitante de un certificado, 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.
- Disponer de un servicio de atención a titulares y terceros, que permita evacuar las consultas y la pronta solicitud de revocación de certificados.
- 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 la Autoridad de Aplicación.
- Abstenerse de generar, exigir, tomar conocimiento o acceder bajo ninguna circunstancia a la clave privada del suscriptor.
- Informar a la Autoridad de Aplicación de modo inmediato la ocurrencia de cualquier evento que comprometa la correcta prestación del servicio.
- Respetar el derecho del titular del certificado a no recibir publicidad de ningún tipo por su intermedio, salvo consentimiento expreso de éste.
- Publicar en el Boletín Oficial durante UN (1) día, el certificado de clave pública correspondiente a la política para la cual obtuvo licenciamiento;
- Cumplir las normas y recaudos establecidos para la protección de datos personales.
- 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 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 haya dejado de ser seguro por razones atribuibles a su titular, el certificador licenciado no estará obligado a sustituir el certificado.
- Enviar periódicamente a la Autoridad de Aplicación, informes de estado de operaciones con carácter de declaración jurada.
- Contar con personal idóneo y confiable, con antecedentes profesionales acordes a la función desempeñada.
- Responder a los pedidos de informes por parte de un tercero respecto de la validez y alcance de un certificado emitido por él.

- Ser responsable con los alcances establecidos en la Ley Nº 25.506, aún en el caso de que delegue parte de su operatoria en Autoridades de Registro, sin perjuicio del derecho del certificador de reclamar a la Autoridad de Registro las indemnizaciones por los daños y perjuicios que aquél sufriera como consecuencia de los actos y/u omisiones de ésta.

c) La obligatoriedad de notificar a sus suscriptores ante cualquier acontecimiento que pudiera ocasionar el compromiso de su clave privada y la generación de un nuevo par de claves

d) La obligatoriedad de notificar a sus suscriptores y a la Autoridad de Aplicación acerca del cese de sus actividades

e) La obligatoriedad de emitir y distribuir los certificados a sus suscriptores, informándolos acerca de dicha emisión

f) Las obligaciones establecidas en la Decisión Administrativa 6/2007 y sus Anexos

g) El cumplimiento de todas las medidas de seguridad establecidas en su Política de Seguridad

2.1.2. - Obligaciones de la Autoridad de Registro

Son obligaciones de la Autoridad de Registro cumplir con:

J.G.M. PRODESPA Nº 3303

a) Las previsiones establecidas en el articulo 35 del Decreto Nº 2628/02

- La recepción de las solicitudes de emisión de certificados.
- La validación de la identidad y autenticación de los datos de los titulares de certificados.
- La validación de otros datos de los titulares de certificados que se presenten ante ella cuya verificación delegue la ANSES.
- La remisión de las solicitudes aprobadas a la ANSES.
- La recepción y validación de las solicitudes de revocación de certificados; y su direccionamiento a la ANSES.
- La identificación y autenticación de los solicitantes de revocación de certificados.
- El archivo y la conservación de toda la documentación de respaldo del proceso de validación de identidad, de acuerdo con los procedimientos establecidos por la ANSES.
- El cumplimiento de las normas y recaudos establecidos para la protección de datos personales.
- El cumplimiento de las disposiciones que establezca la Política de Certificación y el Manual de Procedimientos de la ANSES, en la parte que resulte aplicable.

b) La protección de sus claves privadas

c) El cumplimiento de todas las medidas de seguridad establecidas por la ANSES en el documento anexo "Pautas para la Autoridad de Registro".

2.1.3. - Obligaciones de los suscriptores de los certificados

Son obligaciones de los suscriptores de certificados cumplir con:

a) Las previsiones establecidas en el articulo 25 de la Ley Nº 25.506

- Mantener el control exclusivo de sus datos de creación de firma digital, no compartirlos, e impedir su divulgación;
- Utilizar un dispositivo de creación de firma digital técnicamente confiable;
- 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;
- Informar sin demora al certificador licenciado el cambio de alguno de los datos contenidos en el certificado que hubiera sido objeto de verificación.

b) Proveer de modo completo y preciso toda la información necesaria para la emisión del certificado

c) Utilizar sus certificados de forma adecuada, conforme a lo previsto en la Política de Certificación

d) Tomar conocimiento de los derechos y obligaciones que se establezcan en la "Política de Certificación", en el "Manual de Procedimientos de Certificación" (en sus aspectos no confidenciales), en el "Acuerdo con Suscriptor" y en todo documento aplicable.

e) Solicitar la revocación de su certificado en caso de ocurrir algún cambio que lo excluya de la aplicación de la presente política, como por ejemplo, la finalización de la relación laboral con la ANSES.

2.1.4. - Obligaciones de los terceros usuarios

Son obligaciones de los terceros usuarios de certificados:

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.

2.1.5. - Obligaciones del servicio de repositorio

Son obligaciones del servicio de publicación y repositorio de la ANSES cumplir con:

a) Las previsiones establecidas en el articulo 21 inc. k) de la Ley N° 25.506

- 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, la política 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;

b) Las previsiones establecidas en el articulo 34 incisos g), h) y m) del Decreto N° 2628/02.

- 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 la Autoridad de Aplicación.

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

c) 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

En un todo de acuerdo con la Ley N° 25.506 de Firma Digital, Capítulo IX, existirán dos supuestos de responsabilidad civil:

1) La existente entre este certificador licenciado que emite un certificado respecto del titular de dicho certificado.

   Sin perjuicio de las previsiones de la citada ley, y demás legislación vigente, la relación entre la ANSES y el titular de un certificado emitido por ANSES se regirá por el contrato o acuerdo de partes que se celebre a tal efecto. En este sentido, de acuerdo al artículo 37 de la Ley de Firma Digital la relación quedará encuadrada dentro del ámbito de responsabilidad civil contractual.

   La ANSES no se hace responsable por los daños y perjuicios que hubieran acontecido por culpa de un tercero, de la víctima, o la presencia de un hecho fortuito o de fuerza mayor que no le sea imputable, quedando eximido de resarcir total o parcialmente los daños causados a la víctima en caso de que probara su falta de culpa, o que actuó diligentemente.

   En caso de comprobarse la falta de diligencia, por parte de esta ADMINISTRACIÓN NACIONAL, de acuerdo a lo dispuesto por los artículos 520 y 521 del Código Civil, se deberá proceder a indemnizar los daños y perjuicios que sean consecuencia inmediata del hecho dañoso.

2) La que podría presentarse entre ANSES y un tercero.

   Con respecto a la responsabilidad de esta ANSES por actos que pudieran afectar los intereses de un tercero, en el marco de la presente operatoria, será responsable por los daños y perjuicios que provoque, por los incumplimientos, las imprevisiones, por los errores u omisiones que presenten los certificados digitales que expida, por no revocarlos en legal tiempo y forma y, por las consecuencias imputables a la inobservancia de procedimientos de certificación pertinentes. De acuerdo con el artículo 38 de la Ley N° 25.506.

   Dado que ANSES no esta contratando con terceros la responsabilidad civil será de carácter extra contractual.

J.G.M. PRODESPA II° 3303 7 663

Limitaciones

Se excluye la responsabilidad civil de la ANSES, en un todo de acuerdo con el artículo 39 de la ley 25.506, en los siguientes casos:

- Por las condiciones de emisión y utilización de sus certificados, que no estén expresamente previstos en la ley;
- Por los daños y perjuicios que resulten del uso no autorizado de un certificado;
- Por eventuales inexactitudes en el certificado que resulten de la información facilitada por el titular.

Ninguna de las partes podrá considerar a la otra como responsable por cualquier finalización, interrupción o demora en el cumplimiento de sus obligaciones conforme al presente instrumento que resultara como consecuencia de aquellas causales consideradas como fuerza mayor o caso fortuito (de acuerdo al Código Civil), siempre y cuando la parte que la invocare haya puesto prontamente en conocimiento de la otra parte de manera comprobable y fehaciente las circunstancias del hecho, dentro de las 24 horas de conocido el mismo, y haya tomado las medidas que razonablemente que resultan necesarias, bajo las circunstancias, para mitigar los efectos ocasionados por el hecho de fuerza mayor invocado.

Si se comprobara hecho dañoso se deberá indemnizar a la víctima, de acuerdo a lo estipulado en los artículos 520 y 521 del Código Civil, los daños y perjuicios que sean consecuencia inmediata de dicho hecho.

Cabe destacar que estas disposiciones del Código Civil serán aplicables en forma supletoria a lo establecido expresamente por las partes en el contrato.

2.3. - Responsabilidad Financiera

2.3.1. - Responsabilidad financiera del certificador

Cuando ANSES emite un certificado digital o bien lo reconozca en los términos del artículo 16 de la Ley 25.506 de Firma Digital, será responsable por los daños y perjuicios que provoque, por los incumplimientos a las previsiones de ésta, por los errores u omisiones que presenten los certificados digitales que expide, 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 a la ANSES demostrar que actuó con la debida diligencia, de acuerdo con el artículo 38 de la mencionada Ley.

J.G.M. PRODESPA Nº 3303

2.4. - Interpretación y aplicación de las normas

2.4.1. - Legislación aplicable

La presente Política de Certificación se rige por la Ley 25.506, el Decreto Reglamentario N° 2628/2002 y la Decisión Administrativa 6/2007 de la Jefatura de Gabinete de Ministros y demás normas concordantes dictadas por la autoridad competente.

2.4.2. - Forma de Interpretación y aplicación

Si se presentasen conflictos de interpretación de una o más disposiciones de esta Política de Certificación, el suscriptor o tercero usuario deberán agotar la vía administrativa con jurisdicción en esta ADMINISTRACIÓN, luego de cumplida esta instancia podrá accionar ante la Autoridad de Aplicación.

2.4.3. - Procedimientos de resolución de conflictos

Se deja constancia de que cualquier controversia y/o conflicto resultante de la aplicación de esta Política de Certificación, podrá ser resuelta en sede administrativa de acuerdo a lo establecido por la Ley Nacional de Procedimientos Administrativos N° 19.549 y su Decreto Reglamentario N° 1759/72, y que la presente Política se encuentra supeditada a la normativa vigente en materia de Firma digital (Ley N° 25.506 y sus disposiciones reglamentarias) y que en ningún caso prevalecerá sobre lo dispuesto por ella.

2.5. -Aranceles

Los certificados emitidos bajo la presente política son gratuitos y no se aplica ningún tipo de arancel o tasa por su solicitud, emisión, renovación, revocación o utilización.

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

2.6.1. - Publicación de información del certificador

Se mantiene un repositorio en línea accesible durante las 24hs los 7 días de la semana en las siguientes direcciones:

http://intranetanses/firmadigital

https://servicioswww.anses.gov.ar/firmadigital

La ANSES publica las versiones vigentes de los siguientes documentos:

a) Acuerdo con Suscriptores

b) Política de Privacidad

c) Términos y condiciones con Terceros Usuarios

d) Manual de Procedimientos de Certificación en su parte pública, en sus versiones anteriores y vigente.

e) Política de Certificación, en sus versiones anteriores y vigente.

f) Resumen de la Política de Certificación y del Manual de Procedimientos de Certificación, en su versión corriente y anteriores.

g) Certificado de la "Autoridad Certificante Raíz de la República Argentina" (ACR RA)

h) Certificado de la "Autoridad Certificante para Personas Físicas de la ANSES"

i) Lista de Certificados Revocados (CRL) de la "Autoridad Certificante para Personas Físicas de la ANSES"

j) Información relevante de los informes de la última auditoría realizada por la Autoridad de Aplicación.

J.G.M. PRODESPA Nº 3303

2.6.2. - Frecuencia de publicación

Producida una actualización de los documentos relacionados con el marco legal u operativo de la Autoridad Certificante ("Acuerdo con Suscriptores", "Política de Privacidad", "Términos y condiciones con Terceros Usuarios", "Resumen de la Política de Certificación y del Manual de Procedimientos de Certificación", "Política de Certificación"), los documentos actualizados se publicarán dentro de las VEINTICUATRO (24) horas, luego de ser aprobados por la Autoridad de Aplicación.

Asimismo, toda vez que se produzca una revocación, la Autoridad Certificante para Personas Físicas de la ANSES emite una lista de certificados revocados actualizada en un plazo máximo de VEINTICUATRO (24) horas de aceptado el requerimiento de revocación . Dicha lista indica claramente la fecha y hora de la última actualización.

2.6.3. - Controles de acceso a la información

No se establecen restricciones al acceso de los sitios de publicación de documentación citada en el punto 2.6.1. Los suscriptores que acceden a la Intranet de ANSES deberán hacerlo a través de su identificación de acceso a la red de la Organización.

2.6.4. - Repositorios de certificados y listas de revocación

Los repositorios de información y la publicación de la Lista de Certificados Revocados son administrados en forma directa por la ANSES.

2.7. – Auditorías

La Autoridad de Aplicación de Firma Digital de la República Argentina realiza auditorías ordinarias a la "Autoridad Certificante para Personas Físicas de la ANSES" y a su Autoridad de Registro, a fin de verificar el cumplimiento de los requisitos de licenciamiento.

Las auditorías realizadas tienen por objeto verificar el cumplimiento de los requisitos exigidos para obtener la condición de certificadores licenciados y la aplicación de las políticas y procedimientos aprobados por la Autoridad de Aplicación para la presente política de certificación.

J.G.M. PRODESPA Nº 3303

La ANSES cuenta con una Unidad de Auditoría Interna, que realizará periódicamente la verificación del cumplimiento de los requisitos fijados en la presente Política de Certificación. Asimismo organismos como SIGEN y AGN, realizarán auditorías periódicas.

Siendo los temas principales a evaluar en dichas auditorías:

a) Requisitos legales generales
b) Política de Certificación y Manual de Procedimientos de Certificación
c) Plan de Seguridad
d) Plan de Cese de Actividades
e) Plan de Contingencia
f) Plataforma Tecnológica
g) Ciclo de vida de las claves criptográficas del certificador
h) Ciclo de vida de los certificados de suscriptores
i) Estructura y contenido de los certificados y CRLs
j) Mecanismos de acceso a la documentación publicada, certificados y CRLs
k) Pautas para la Autoridad de Registro.

En caso de producirse observaciones en las auditorías realizadas luego de la notificación a la máxima autoridad de ANSES, se tomarán a la brevedad las medidas correctivas de carácter legal y técnico que amerite el caso.

En cumplimiento del artículo 21 Inciso K de la Ley Nº 25.506, la información relevante de los informes de la última auditoría realizada por la Autoridad de Aplicación, es publicada en los sitios mencionados en el apartado "2.6.1. - Publicación de información del certificador".

2.8. - Confidencialidad

Todos los datos correspondientes a las personas físicas a las cuales alcance esta Política de Certificación están sujetos a la Ley N° 25.326 de Protección de los Datos Personales.

Como principio general, se establece que toda información remitida por el solicitante de un certificado al momento de efectuar un requerimiento debe ser considerada confidencial y no ser divulgada a terceros sin el consentimiento previo del solicitante o suscriptor, salvo que sea requerida en causa judicial por un juez competente.

Esta exigencia se extiende a toda otra información referida a los solicitantes y suscriptores de certificados a la que tenga acceso la ANSES o la AR durante el ciclo de vida del certificado.

2.8.1. - Información confidencial

La protección abarca a la siguiente información, en la medida en que no sea de conocimiento público:

- Toda la información remitida por el solicitante o suscriptor a la Autoridad de Registro.
- Cualquier información almacenada en servidores o bases de datos destinadas a Firma Digital de esta Administración Nacional.
- Cualquier información impresa o transmitida en forma verbal referida a procedimientos, manual de procedimientos, etc., salvo aquellos que en forma expresa fueran declarados como no confidenciales.
- Cualquier información referida a planes de contingencia, controles o procedimientos de Seguridad, registros de auditoría creados y/o mantenidos por ANSES.
- La presente es de carácter enunciativo, resultando confidencial toda información del proceso de Firma Digital, que expresamente no señale lo contrario.

J.G.M.
PRODESPA Nº
3303
7

Esta Administración Nacional se compromete, a la hora de prestar sus servicios de certificación, a publicar exclusivamente los datos del suscriptor imprescindibles para el reconocimiento de su firma digital.

A los efectos de lo dispuesto en la normativa citada, se informa al solicitante o suscriptor de la existencia de certificados revocados. ANSES, como responsable de dicha lista, se compromete a poner los medios a su alcance para evitar la alteración, pérdida, tratamiento o acceso no autorizado a los datos de carácter personal contenidos en ese listado. Asimismo, se informa al solicitante o suscriptor sobre el derecho que le asiste a acceder o rectificar sus datos de carácter personal siempre que se aporte la documentación necesaria para ello.

Toda información que no sea considerada como pública revestirá el carácter de confidencial, declarándose expresamente como tal a:

La clave privada de la Autoridad Certificante:

- La Autoridad Certificante garantiza la confidencialidad frente a terceros de su clave privada, la cual, al ser el punto de máxima confianza será generada y custodiada conforme a lo que se especifique en la presente política.

Las claves privadas del solicitante o suscriptor:

- Para garantizar la confidencialidad de las claves de autentificación y firma del solicitante o suscriptor, esta Administración Nacional proporcionará los medios para que la generación de dichas claves sólo se realice de modo seguro a través de un dispositivo criptográfico. Dichas claves serán generadas por el propio solicitante y almacenadas en un dispositivo criptográfico. A su vez, tanto la Autoridad de Registro (AR) como la Autoridad Certificante (AC) no tendrán la posibilidad de almacenar, copiar o conservar cualquier tipo de información que sea suficiente para reconstruir estas claves ni activarlas.

2.8.2. - Información no confidencial

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

a) Acuerdo con Suscriptores

b) Política de Privacidad

c) Términos y condiciones con Terceros Usuarios

d) Manual de Procedimientos de Certificación en su parte pública.

e) Política de Certificación.

f) Resumen de la Política de Certificación y del Manual de Procedimientos de Certificación.

g) Certificado de la "Autoridad Certificante Raíz de la República Argentina" (ACR RA)

h) Certificado de la "Autoridad Certificante para Personas Físicas y Jurídica de la ANSES"

i) Lista de Certificados Revocados (CRL) de la "Autoridad Certificante para Personas Físicas de la ANSES"

j) Información relevante de los informes de la última auditoría realizada

J.G.M. PRODESPA Nº 3303

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

No serán consideradas de carácter confidencial las listas de certificados revocados.

La ley 25506 no admite la suspensión de certificados.

2.8.4. - Divulgación de información a autoridades judiciales

La ANSES podrá revelar información confidencial si es requerida por autoridad judicial y conforme las condiciones de dicho requerimiento.

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

La ANSES podrá revelar información confidencial si es requerida en el marco de procesos judiciales, administrativos u otros procesos legales, tales como citaciones, interrogatorios o solicitud de pruebas.

2.8.6. - Divulgación de información por solicitud del suscriptor

De acuerdo al artículo 14 de la Ley Nº 25.326 de Protección de los Datos Personales, el titular de los datos, previa acreditación de su identidad, tiene derecho a solicitar y obtener información respecto de los datos que sobre su persona obren en los bancos de datos públicos,

y de acuerdo con las condiciones establecidas en esta ley. En este caso se preverá que el acceso a la lectura de información de la Base de Datos de Firma Digital esté circunscrito a los datos personales del suscriptor y solo a ellos.

2.8.7. - Otras circunstancias de divulgación de información

La ANSES no divulgará información confidencial a terceros bajo ninguna otra circunstancia que las previstas en los apartados anteriores, excepto en los casos de excepción previstos en el artículo 11 de la Ley N° 25.326 de Protección de los Datos Personales.

2.9. - Derechos de Propiedad Intelectual

La ANSES es propietaria exclusiva de todos los derechos de propiedad intelectual de la presente política, acuerdos, declaraciones, procedimientos y documentos auxiliares referidos a la Autoridad Certificante para Personas Físicas de la ANSES, así como la documentación y contenidos de los sitios:

- http://intranetanses/firmadigital
- https://servicioswww.anses.gov.ar/firmadigital

y de las aplicaciones informáticas propias, exceptuando software de base y su correspondiente documentación.

J.G.M.
PRODESPA N°
3303
87

3. - IDENTIFICACION Y AUTENTICACION

3.1. - Registro inicial

3.1.1. -Tipos de Nombres

No se establecen restricciones a los nombres que pueden ser incluidos dentro de los certificados, en tanto se correspondan con la documentación probatoria exigida para la emisión de certificados por esta política.

3.1.2. - Necesidad de Nombres Distintivos

Los siguientes atributos son incluidos en los certificados e identifican unívocamente al suscriptor:

"*commonName*" (OID 2.5.4.3: Nombre común):

Se corresponde exactamente con el nombre que figura en el documento de identidad del suscriptor.

"*serialNumber*" (OID 2.5.4.5: Número de serie):

Contiene el número de CUIL del titular. El campo se representa bajo el formato: "CUIL [número de CUIL]"

"*description*" (OID 2.5.4.13: Descripción):

Contiene la identificación del suscriptor (userID) en la red interna de la ANSES.

"*emailAddress*" (OID 1.2.840.113549.1.9.1: Correo electrónico):

Está presente en todos los certificados y contiene la dirección de correo electrónico del suscriptor dentro de la ANSES.

"*title*" (OID 2.5.4.12: Título):

En caso de estar presente en el certificado identifica el rol o función asignada al suscriptor dentro de la ANSES. Este atributo se encuentra funcionalmente vinculado con los siguientes atributos:

"*organizationalUnitName*" (OID 2.5.4.11: Nombre de la suborganización):

En caso de estar presente en el certificado, identifica en que área se desempeña el suscriptor. Pueden existir varías ocurrencias de este atributo, representando la dependencia jerárquica de las áreas dentro de la organización.

"*organizationName*" (OID 2.5.4.10: Nombre de la organización):

Debido a que la presente política esta destinada al personal que preste servicios a ANSES y quienes la representen en el ámbito externo de la Organización, este atributo contiene "Administración Nacional de Seguridad Social" en todos los certificados.

"*localityName*" (OID 2.5.4.7: Localidad):

J.G.M. PRODESPA Nº 3303 7

En caso de estar presente en el certificado identifica la localidad donde desempeña funciones el suscriptor. Este atributo se encuentra funcionalmente vinculado con los dos siguientes atributos (Provincia y Código de país).

"*stateOrProvinceName*" (OID 2.5.4.8: Provincia):

En caso de estar presente en el certificado identifica la provincia donde desempeña funciones el suscriptor.

"*countryName*" (OID 2.5.4.6: Código de país):

Debido a que los suscriptores de la presente política desempeñan funciones dentro de la ANSES este campo contiene "AR" en todos los certificados.

3.1.3. - Reglas para la interpretación de nombres

Todos los nombres representados dentro de los certificados emitidos bajo la presente política coinciden con los del correspondiente documento personal. En casos de coincidencia de nombres, el método de resolución será la combinación del "Nombre común" con los atributos "Número de serie" y "Descripción".

3.1.4. - Unicidad de nombres

El nombre distintivo de cada certificado es único para cada suscriptor.

Si dos o más suscriptores tuvieran el mismo nombre y apellido, la unicidad queda resuelta por medio de los atributos citados en el punto 3.1.3.

3.1.5. - Procedimiento de resolución de disputas sobre nombres

La ANSES se reserva el derecho de tomar todas las decisiones referidas a posibles conflictos sobre la utilización y titularidad de cualquier nombre en los certificados de sus suscriptores.

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

No aplica por tratarse de una Política de Certificación de personas físicas.

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

Para la comprobación de la posesión de la clave privada se utiliza el siguiente procedimiento:

a) El solicitante es partícipe directo y necesario para la generación de su par de claves criptográficas asimétricas.

b) Durante el proceso de solicitud, el solicitante es requerido para la generación de un par de claves criptográficas asimétricas.

c) Las claves son generadas y almacenadas en dispositivos criptográficos.

d) Los datos de la solicitud y el requerimiento con la clave pública del solicitante, en formato PKCS#10, son enviados a la aplicación de la Autoridad Certificante.

e) La aplicación de la Autoridad Certificante valida el requerimiento PKCS#10.

f) En caso de ser correcto el formato, la aplicación de la Autoridad Certificante entrega al solicitante un "recibo de solicitud" incluyendo el resumen criptográfico (huella SHA-1).

g) El solicitante deberá tomar nota y proceder a la conservación del PIN "de revocación" informado por la aplicación de la Autoridad de Certificación. El PIN "de revocación" es un valor único y se compone del resumen criptográfico (huella SHA-1) y del número de solicitud de emisión.

h) El solicitante debe imprimir el "recibo de solicitud" para entregar a la Autoridad de Registro en el proceso de identificación y autenticación.

J.G.M. PRODESPA Nº 3303

La aplicación de la Autoridad Certificante, una vez que emita el certificado, eliminará automáticamente el requerimiento PKCS#10 asociado a ese certificado con el fin de evitar que se genere un nuevo certificado con dicho requerimiento.

3.1.8. - Autenticación de la identidad de personas físicas

El proceso de solicitud debe ser iniciado exclusivamente por el solicitante, accediendo a la aplicación de la Autoridad Certificante para Personas Físicas de la ANSES.

El solicitante debe presentarse personalmente frente a la Autoridad de Registro habilitada donde acreditará fehacientemente su identidad, acompañando la siguiente documentación:

a) Documento de Identidad y fotocopia:

- Documento Nacional de Identidad o
- Libreta de Enrolamiento o
- Libreta Cívica

b) Nota de Autorización (original y copia), dirigida al responsable de la Autoridad de Registro y consignando los siguientes datos:

- Motivos o causas por los cuales requiere un certificado de la AC-ANSES.
- Tipo y Número de Documento de Identidad.
- Área a la que pertenece: Jurisdicción, Organismo, Dependencia y Cargo.

- Firma del máximo responsable del área.
- Certificación por la Mesa de Entradas, Salidas y Archivo.

c) Recibo de solicitud, impreso.

La Autoridad de Registro verificará la identidad del solicitante, la documentación que presenta y el resumen criptográfico (huella SHA-1) vinculada con la solicitud, así como toda otra información contenida en la solicitud.

Posteriormente, la aceptación o rechazo de la solicitud será informada al solicitante por correo electrónico y también podrá consultarse su estado a través de la aplicación de la Autoridad Certificante.

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

En caso de que el suscriptor requiera generar un nuevo par de claves deberá realizar el proceso de solicitud completo, incluyendo el envío de la solicitud y la presentación frente a la Autoridad de Registro para validar su identidad.

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

En caso de que el suscriptor requiriera generar un nuevo par de claves deberá realizar el proceso de solicitud completo, incluyendo el envío de la solicitud y la presentación frente a la Autoridad de Registro para validar su identidad.

3.4. - Requerimiento de revocación

La revocación podrá ser iniciada por el Suscriptor y la Autoridad de Registro.

Los suscriptores podrán solicitar la revocación de su certificado de la siguiente forma:

a) Ingresando a la aplicación de la Autoridad de Certificante desde:

   http://intranetanses/firmadigital

   Selecciona el certificado a revocar y envía la solicitud. En este caso, la identificación se realizará utilizando las credenciales de usuario de red y será suficiente para aceptar la solicitud de revocación.

b) Ingresando a la aplicación de la Autoridad de Certificante desde:

   https://servicioswww.anses.gov.ar/firmadigital

   Se identifica con su usuario de red (userID) y como password ingresa el PIN de "revocación" y procede a enviar la solicitud.

c) Presentándose personalmente ante la Autoridad de Registro, en este caso quedará asentado en un Libro de Actas de la Autoridad de Registro.

La Autoridad de Registro podrá iniciar de oficio la revocación de certificados, según lo indicado en el "4.4.1. - Causas de revocación".

La Autoridad de Registro procede a ingresar a la aplicación de la Autoridad Certificante, selecciona el certificado perteneciente al suscriptor y procede a la revocación.

4. - CICLO DEL CERTIFICADO: REQUERIMIENTOS OPERATIVOS

4.1. - Solicitud de certificado

4.1.1. - Solicitud de emisión

El proceso de solicitud de emisión de certificado debe ser iniciado exclusivamente por el solicitante, quien debe acreditar fehacientemente su identidad según se indica en "3.1.8. - Autenticación de la identidad de personas físicas".

Para poder efectuar la solicitud de un certificado, los solicitantes deben:

a) Estar conectados a la red interna y haber iniciado sesión en el dominio de ANSES

b) Utilizar un sistema operativo Windows 2000, XP o superior

c) Utilizar Internet Explorer versión 6.0 o superior como navegador

d) Estar autorizado para acceder a la aplicación de la Autoridad Certificante.

e) Poseer un dispositivo criptográfico inicializado, operativo y con controladores instalados.

J.G.M. PRODESPA N° 3303

Para iniciar el pedido de emisión del certificado, el solicitante debe ingresar al sitio Intranet de ANSES y seleccionar el enlace a la aplicación de la Autoridad Certificante.

La aplicación de la Autoridad Certificante verifica que la estación de trabajo del solicitante cumple con los requerimientos técnicos mínimos y presenta la pantalla del proceso de solicitud y a continuación muestra el "Acuerdo con Suscriptores".

El solicitante deberá aceptar el "Acuerdo con Suscriptores" para poder continuar con el proceso.

La aplicación de la Autoridad Certificante, utilizando la identificación del usuario con sesión activa en la estación de trabajo, obtendrá la información personal y laboral desde las bases de datos de Recursos Humanos de esta Administración Nacional.

La siguiente información es presentada al solicitante para su verificación:

a) UserID,

b) Apellidos y Nombres,

c) E-mail

d) CUIL

e) Cargo

f) Dependencia y Área

g) Localidad y Provincia

h) Observaciones

El solicitante deberá verificar los datos presentados.

En caso de ser incorrectos los datos, no podrá continuar con la solicitud, debiendo comunicarse con el área de Recursos Humanos para actualizar sus datos.

En casos de ser los datos correctos, el solicitante completa los campos del formulario habilitados, selecciona la opción "Enviar" y se genera un nuevo par de claves, luego de lo

cual, la aplicación de la Autoridad Certificante remite los datos de la solicitud y el requerimiento con la clave pública del solicitante, en formato PKCS#10.

La aplicación de la Autoridad Certificante entrega al solicitante un "recibo de solicitud" incluyendo el resumen criptográfico (huella SHA-1).

El solicitante deberá tomar nota y proceder a la conservación del PIN "de revocación" informado por la aplicación de la Autoridad de Aplicación.

El solicitante deberá imprimir el "recibo de solicitud" para entregar a la Autoridad de Registro en el proceso de identificación y autenticación.

Luego, la aplicación de la Autoridad Certificante, envía notificaciones de correo electrónico a los siguientes actores:

a) Al solicitante, a los efectos de informar la documentación a entregar ante la Autoridad de Registro según lo indicado en "3.1.8. - Autenticación de la identidad de personas físicas" y los plazos para presentarse.

b) A la Autoridad de Registro, a fin de informar una nueva solicitud de emisión.

El proceso continúa como se describe en "4.2. - Emisión del certificado".

J.G.M. PRODESPA IP 3303

4.1.2. - Solicitud de renovación

El proceso de solicitud de renovación es iniciado exclusivamente por el suscriptor antes de vencer el periodo de validez de su certificado. El periodo de validez es indicado en "6.3.2.- Periodo de uso de la clave pública y privada". En el caso de que el certificado hubiera expirado, el suscriptor deberá iniciar una solicitud de renovación de certificado, siguiendo lo expresado en el "4.1.1.- Solicitud de emisión".

Para iniciar la solicitud de renovación de su certificado, el suscriptor deberá ingresar al sitio Intranet de la ANSES y seleccionar el enlace a la aplicación de la Autoridad Certificante.

La aplicación de la Autoridad Certificante verificará que la estación de trabajo del suscriptor cumple con los requerimientos técnicos mínimos (según lo indicado en 4.1.1) y presenta la pantalla del proceso de solicitud de renovación.

El suscriptor deberá seleccionar el certificado a renovar para poder continuar con el proceso.

La aplicación de la Autoridad Certificante, utilizando la identificación del usuario, con sesión activa en la estación de trabajo, obtiene la información del certificado desde la base de datos de los certificados de esta Administración Nacional.

El suscriptor deberá verificar los datos presentados por la aplicación.

En caso de que los datos sean incorrectos, no podrá continuar con la solicitud de renovación y, si así correspondiera, pasar al proceso de solicitud de revocación según el apartado "4.4.3. - Procedimientos para la solicitud de revocación", por encontrarse vigente el certificado y luego iniciar una nueva solicitud de emisión de certificado siguiendo lo expresado en el "4.1.1.- Solicitud de emisión".

En caso de ser los datos correctos, el suscriptor selecciona la opción "Enviar" y se genera un nuevo par de claves, luego de lo cual la aplicación de la Autoridad Certificante recibirá los datos de la solicitud y el requerimiento con la clave pública del suscriptor, en formato PKCS#10.

La aplicación de la Autoridad Certificante entrega al suscriptor un "recibo de solicitud de renovación" incluyendo el resumen criptográfico (huella SHA-1).

El suscriptor deberá tomar nota y conservar el PIN "de revocación" informado por la aplicación de la Autoridad de Certificación.

El suscriptor deberá imprimir y resguardar el "recibo de solicitud de renovación" como respaldo de la acción realizada.

La aplicación de la Autoridad Certificante, envía notificaciones de correo electrónico, a los siguientes actores:

a) Al suscriptor, a los efectos de informar que fue ingresada al circuito de evaluación.

b) A la Autoridad de Registro, a fin de informar de una nueva solicitud de renovación.

La Autoridad de Registro deberá verificar los datos de la solicitud de renovación, comparándolos con los oportunamente presentados con la documentación indicada en "3.1.8. - Autenticación de la identidad de personas físicas". El proceso continúa como se describe en "4.2. - Emisión del certificado".

J.G.M. PRODESPA Nº 3303 7

4.2. - Emisión del certificado

Cumplidos los recaudos del proceso de identificación y autenticación de acuerdo con esta Política y una vez completada y aprobada la solicitud por la Autoridad de Registro, la aplicación de la Autoridad Certificante emite el correspondiente certificado, firmándolo digitalmente con su clave privada. Posteriormente, el certificado está disponible al suscriptor como un archivo adjunto de un correo electrónico y/o a través de la aplicación de la Autoridad Certificante.

4.3. - Aceptación del certificado

Una vez notificado de la emisión de un certificado a su nombre, el suscriptor deberá controlar su contenido y dar su conformidad para proceder a la instalación y posterior utilización.

En caso de que existiera algún error u omisión en los datos del suscriptor contenidos en el certificado, deberá informarlo inmediatamente a la Autoridad de Registro para que ésta proceda a su revocación.

Con la aceptación del certificado, el suscriptor confirma y asume la exactitud del contenido del mismo, aceptando la totalidad de las obligaciones y responsabilidades establecidas por esta Política de Certificación para Personas Físicas de la ANSES.

4.4. - Suspensión y Revocación de Certificados

El estado de suspensión no es admitido en el marco de la Ley Nº 25.506.

4.4.1. - Causas de revocación

La Autoridad Certificante para Personas Físicas de la ANSES revocará un certificado en los casos en que:

a) Lo solicite su titular.

b) Lo solicite el titular por tomar conocimiento de que su clave privada estuviera comprometida y hubiera dejado de ser segura.

c) La ANSES determine que el certificado fue emitido en base a una información falsa, que en el momento de la emisión hubiera sido objeto de verificación.

d) La ANSES determine que los procedimientos de emisión y/o verificación han dejado de ser seguros.

e) La ANSES determine que la información contenida en el certificado ha dejado de ser exacta o casos tales como: renuncia o despido del suscriptor, fallecimiento o enfermedad prolongada del suscriptor, adscripción del suscriptor a otro organismo, licencia por cargo de mayor jerarquía, licencia por razones personales, entre otros.

f) Lo solicite el máximo responsable del área a la que pertenece el suscriptor o la máxima autoridad de ANSES, con la debida justificación.

g) Se solicite por resolución judicial o de la Autoridad de Aplicación de la Ley N° 25.506 debidamente fundada.

h) La ANSES determine que el certificado dejó de cumplir con las políticas y normas legales y reglamentarias de la Infraestructura de Firma Digital de la República Argentina (IFDRA).

J.G.M. PRODESPA N° 3303

4.4.2. - Autorizados a solicitar la revocación

Las siguientes personas podrán presentar el pedido de revocación ante la Autoridad de Registro:

a) El suscriptor del certificado.

b) El máximo responsable del área a la que pertenece el suscriptor.

c) La Autoridad de Registro

d) La máxima autoridad de ANSES

e) La Autoridad de Aplicación

f) La Autoridad Judicial competente

4.4.3. - Procedimientos para la solicitud de revocación

Para solicitar la revocación de su certificado, el suscriptor seguirá lo indicado en el apartado "3.4. - Requerimiento de revocación"

La Autoridad de Registro y la Autoridad Certificante conservarán como documentación probatoria toda solicitud de revocación y el material probatorio vinculado.

Los suscriptores serán notificados en sus respectivas direcciones de correo electrónicos del cumplimiento del proceso de revocación.

4.4.4. - Plazo para la solicitud de revocación

La recepción de la solicitud de revocación está disponible 7 x 24 hs. a través de la aplicación de la Autoridad Certificante y esa solicitud será procesada de inmediato.

En caso de que el suscriptor se presente personalmente ante la Autoridad de Registro, la revocación también es inmediata.

Luego de la revocación, se emite y publica en forma inmediata la nueva lista de certificados revocados.

4.4.5. - Causas de suspensión

El estado de suspensión no es admitido en el marco de la Ley Nº 25.506.

4.4.6. - Autorizados a solicitar la suspensión

El estado de suspensión no es admitido en el marco de la Ley Nº 25.506.

4.4.7. - Procedimientos para la solicitud de suspensión

El estado de suspensión no es admitido en el marco de la Ley Nº 25.506.

4.4.8. - Limites del periodo de suspensión de un certificado

El estado de suspensión no es admitido en el marco de la Ley Nº 25.506.

J.G.M. PRODESPA Nº 3303 87

4.4.9. - Frecuencia de emisión de listas de certificados revocados

La Autoridad Certificante para Personas Físicas de la ANSES genera y publica una única lista conteniendo todos los certificados revocados por ella, en formato del CRL X.509 v2, con una frecuencia no mayor a VEINTICUATRO (24) horas.

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

Para determinar el estado de validez de un certificado, se deben obtener la CRL vigente, verificar su integridad controlando la validez de su firma y constatar la inclusión o no del certificado en cuestión.

En los repositorios descriptos en el apartado "2.6.1. - Publicación de información del certificador" se conserva únicamente la última CRL emitida. Las versiones anteriores de CRLs emitidas son mantenidas en los archivos internos de la Autoridad Certificante para Personas Físicas de la ANSES.

Si no se pudiera obtener una CRL actualizada, se deberá optar entre rechazar el documento firmado digitalmente o aceptarlo bajo exclusiva responsabilidad de quien consulta.

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

La ANSES no ofrece servicios de verificación en línea del estado de los certificados.

El único mecanismo válido para la verificación del estado de los certificados es a través de las Listas de Certificados Revocados (CRLs).

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

No aplicable.

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

Todas las situaciones que involucren el compromiso de las claves privadas el suscriptor debe informarlas a la ANSES por alguna de las vías indicadas en el punto "4.4.3. - Procedimientos para la solicitud de revocación"

La ANSES podrá iniciar una investigación para determinar quiénes tuvieron responsabilidad en el hecho, cuál fue el nivel de exposición al riesgo de uso fraudulento de las claves, y podrá aplicar las sanciones y medidas correctivas que resultaren necesarias.

4.5. - Procedimientos de Auditoría de Seguridad

La Autoridad Certificante para Personas Físicas de la ANSES mantiene registros de auditoría de todas las operaciones que realiza, protegiendo su integridad en medios de almacenamiento encriptados y conservándolos por al menos 10 años.

J.G.M. PRODESPA N° 3303

Estos registros de auditoría son utilizados para tareas de monitoreo habitual del funcionamiento de los sistemas y procesos, para posibles auditorías internas por parte de la Unidad de Auditoría Interna de la ANSES y para las auditorías que realiza la Autoridad de Aplicación.

Con el propósito de mantener la seguridad de los sistemas, la Gerencia de Seguridad Informática realiza evaluaciones periódicas de vulnerabilidad de todos los servidores involucrados en el funcionamiento de la Autoridad Certificante.

Asimismo, atendiendo a lo expresado en el punto 2.7 Auditoría, se mantendrán registros no informatizados de toda aquella información.

4.6. - Archivo de registros de eventos

La Autoridad Certificante conserva registro de eventos sobre cada una de las siguientes actividades:

Administración del ciclo de vida de las claves criptográficas	a) Generación y almacenamiento de las claves criptográficas del certificador b) Resguardo y recuperación de las claves criptográficas del certificador c) Utilización de las claves criptográficas del certificador d) Archivo de las claves criptográficas del certificador e) Retiro de servicio de datos relacionados con las claves criptográficas f) Destrucción de claves criptográficas del certificador g) Identificación de la entidad que autoriza una operación de administración de claves criptográficas h) Identificación de la entidad que administra los datos relativos a las claves criptográficas

	i) Compromiso de la clave privada
Administración del ciclo de vida de los certificados	a) Recepción de solicitudes de certificados b) Transferencia de claves públicas para la emisión del certificado c) Cambios en los datos de la solicitud del certificado d) Generación de certificados e) Distribución de la clave pública del certificador f) Solicitudes de revocación de certificados g) Generación y emisión de listas de certificados revocados h) Acciones tomadas en relación con la expiración de un certificado
Administración del ciclo de vida de los dispositivos criptográficos	a) Recepción del dispositivo b) Ingreso o retiro del dispositivo del lugar de almacenamiento c) Instalación del dispositivo d) Uso del dispositivo e) Desinstalación del dispositivo f) Envío de un dispositivo para servicio técnico o reparación g) Retiro, baja o borrado de información del dispositivo
Información relacionada con la solicitud de Certificados	a) Tipos de documentos de identificación presentados por el solicitante b) Ubicación del archivo de las copias de las solicitudes de certificados y de los documentos de identificación c) Identificación de la entidad que recibe y acepta la solicitud d) Método utilizado para validar los documentos de identificación e) Identificación de la Autoridad de Registro
Eventos de seguridad	a) Lecturas y/o escrituras en archivos sensibles de seguridad b) Borrado de datos sensibles de seguridad c) Cambios en los perfiles de seguridad d) Registro de intentos exitosos y fallidos de accesos al sistema, los datos y los recursos e) Caídas del sistema, fallas en el hardware y software, u otras anomalías f) Acciones desarrolladas por los operadores y administradores del sistema y responsables de seguridad g) Cambios en la relación entre la Autoridad Certificante y su Autoridad de Registro o personal relacionado con el proceso de certificación h) Accesos al los componentes del sistema de la Autoridad Certificante

	i) Eventos o situaciones no previstas

4.7. - Cambio de claves criptográficas

Las claves criptográficas de la Autoridad Certificante para Personas Físicas de la ANSES han sido generadas con motivo del licenciamiento de la presente Política de Certificación en presencia de la Autoridad de Aplicación de Firma Digital y tendrán una duración de 10 años. Por su parte, ,la licencia, en sí misma, tiene una vigencia limitada a 5 años.

El cambio del par de claves criptográficas de la Autoridad Certificante para Personas Físicas de la ANSES, dará origen a la emisión de un nuevo certificado, por parte de la AC Raíz de la Autoridad de Aplicación, y será usado para la emisión de los posteriores certificados de los suscriptores. Este certificado estará disponible para su consulta en los sitios web informados.

Dos años antes del vencimiento previsto del certificado de la Autoridad Certificante se realizará una nueva generación de claves y se solicitará la renovación de la licencia de "Certificador Licenciado". Una vez concedida la licencia, la nueva clave pública será distribuida en un certificado firmado por la "Autoridad Certificante Raíz de la República Argentina" (ACR RA).

J.G.M.
PRODESPA Nº
3303
7

4.8. - Plan de contingencia y recuperación ante desastres

El plan de contingencia de la ANSES como certificador licenciado establece los procedimientos y actividades relacionados con el servicio de certificación de Firma Digital y será de aplicación desde el momento de la declaración de la emergencia hasta la restauración de la operatoria normal.

La emergencia será declarada cuando se produzca uno de los siguientes:

a) Revocación de su certificado.

b) Compromiso o sospecha de compromiso de su clave privada.

c) Destrucción del hardware.

d) Destrucción de las fuentes de energía.

e) Siniestro que afecte a la estructura del edificio.

f) Necesidad de continuar las operaciones en un entorno seguro luego de desastres naturales o de otra naturaleza.

g) Pérdida de la capacidad de procesamiento de Hardware y/o Software.

h) Necesidad de recuperación ante falla o sospecha de falla de componentes de hardware, software y datos.

i) Fallas en los sistemas de comunicaciones.

j) Fallas de suministros, como por ejemplo aire acondicionado o líneas de energía eléctrica estabilizada, por periodos extensos.

En casos de emergencia, el Responsable de Contingencia es el encargado de administrar el cumplimiento del Plan de Contingencia.

Declarada la contingencia, se integrará un Comité de Contingencia, que tiene la responsabilidad de dirigir las operaciones de recuperación y restauración del procesamiento normal, de acuerdo a lo detallado en el Plan de Contingencia.

Están previstos mecanismos de prueba y simulación con una periodicidad de SEIS (6) meses o cuando los cambios realizados al hardware, software de base y/o software aplicativo lo ameriten. Las pruebas del plan tienen por objeto brindar los elementos necesarios para minimizar el tiempo de recuperación y contar con información real respecto al servicio de contingencia.

4.9. - Plan de Cese de Actividades

Ante la declaración de cese en la prestación de los servicios de certificación, la ANSES elaboró un Plan de Cese, que contempla las estrategias y procedimientos a seguir desde dicha declaración hasta la inhabilitación lógica y física de la Autoridad Certificante para Personas Físicas de la ANSES.

J.G.M. PRODESPA Nº 3303

La ejecución del Plan de Cese se podrá producir a partir de la manifestación de la máxima autoridad de la ANSES sobre su decisión unilateral de proceder al cese de actividades, ya sea por razones de índole política o de seguridad. También podrá ser motivado por cancelación de la licencia dispuesta por la Autoridad de Aplicación o por disolución de esta Administración Nacional.

Ante la declaración del cese de los servicios de certificación, la ANSES procederá a su publicación a través del Boletín Oficial, del sitio https://servicioswww.anses.gov.ar/firmadigital/, por Gacetilla de Prensa de esta ADMINISTRACIÓN NACIONAL y la publicación en un medio de difusión nacional.

Las acciones previstas para proceder a dicha declaración y aquellas que devienen de ella se encuentran contempladas en el documento interno titulado Plan de Cese de Actividades.

Se mantendrán los registros necesarios para proporcionar prueba cierta de los servicios de certificación, para lo cual se realizarán copias de resguardo de los registros, los cuales serán almacenados en un servidor que opera dentro de instalaciones seguras.

Toda información digital será resguardada por ANSES por un plazo de DIEZ (10) años, así como toda la documentación de respaldo de las solicitudes. Si el cese se debiera a la disolución de este Organismo, los registros pasarán a manos del organismo que se instituya para realizar funciones similares o al Ministerio de Trabajo y Seguridad Social.

5. - CONTROLES DE SEGURIDAD FÍSICA, FUNCIONALES Y PERSONALES

5.1. - Controles de seguridad física

Los sistemas centrales de la Autoridad Certificante para Personas Físicas de la ANSES se encuentran aislados en un compartimiento exclusivo en el interior de la "Sala Cofre" de la ANSES denominado "Recinto de la Autoridad Certificante".

La "Sala Cofre" cuenta con controles de seguridad física que protegen las instalaciones informáticas de la ANSES y garantizan la continuidad de sus operaciones.

Algunas de sus características comprenden:

a) Monitoreo ambiental de temperatura, humedad, ruido, flujo de aire, polvo, polución, etc.

b) Prevención contra agentes naturales como agua, vapor, calor, fuego, gases, polvo, etc.

c) Aislamiento a altas temperaturas externas.

d) Aislamiento a campos magnéticos externos.

e) Estructura sólida de bóveda.

f) Prevención contra explosiones, derrumbes y sismos.

g) Prevención temprana de incendios.

h) Sistemas de extinción de fuego.

i) Sistemas de refrigeración y control de humedad.

j) Sistemas de alimentación eléctrica redundante.

k) Sistemas de suministro de energía ininterrumpido.

l) Sistema de generación de energía alternativo.

m) Sistemas de conectividad redundantes.

n) Sistema de puerta doble con cerramiento automático.

o) Control de acceso con identificación biométrica.

p) Sistema de cámaras para monitoreo completo en accesos y áreas críticas.

J.G.M. PRODESPA II° 3303

El acceso a la Sala Cofre está limitado al personal autorizado y estrictamente necesario para el mantenimiento y administración de los sistemas de la ANSES.

El almacenamiento de los datos de activación de la clave privada de la Autoridad Certificante se realiza en el "Recinto de Autoridad Certificante" cumpliendo con los niveles de seguridad de acceso físico establecidos por la normativa vigente. Las copias de respaldo de sistemas y de datos de la Autoridad Certificante se almacenan debidamente rotuladas en un cofre de seguridad y bajo los niveles de seguridad y autorización dentro del "Recinto de Autoridad Certificante".

5.2. - Controles Funcionales

Los controles funcionales son cumplidos por personal calificado asignando a cada uno de ellos un rol específico para la operación de la Autoridad Certificante para Personas Físicas de la ANSES.

Los roles son asignados por el Responsable de la AC, respetando los siguientes criterios:

a) Cada uno de los roles tiene un titular asignado y, por lo menos, un sustituto.

b) Los roles son asignados a personal que cumple funciones en ANSES.

c) Todos los roles son excluyentes entre si.

5.3. - Controles de seguridad del personal

La Gerencia de Recursos Humanos implementa el análisis y seguimiento de los antecedentes laborales del personal a través de su Curriculum Vitae y evalúa la idoneidad del aspirante mediante una evaluación psico-técnica. De igual manera, ANSES aplica un sistema de

calificación anual de acuerdo a los factores que constan en el CAPÍTULO VIII, ARTÍCULO 34 al ARTÍCULO 46 del Reglamento de Personal y Régimen Disciplinario de ANSES.

5.3.1. - Antecedentes laborales, calificaciones, experiencia e idoneidad del personal

Para cada persona vinculada con los servicios de certificación, la ANSES confecciona un legajo de antecedentes laborales, calificaciones profesionales, experiencia e idoneidad.

Todos los antecedentes personales y profesionales son evaluados antes de la asignación de una persona a un rol en estos servicios.

5.3.2. - Entrenamiento y capacitación inicial

La ANSES realiza cursos de entrenamiento e instrucción en todas las políticas y procedimientos que conforman los manuales operativos de la Autoridad Certificante.

Las sesiones de entrenamiento se orientan a los procedimientos específicos de cada rol e incluyen, entre otros, los siguientes contenidos:

a) Política de Seguridad

b) Política de Certificación

c) Procedimientos específicos correspondientes al rol

d) Planes de contingencia

e) Procedimientos de emergencia y evacuación

J.G.M.
PRODESPA Nº
3303

5.3.3. - Frecuencia de procesos de actualización técnica

Conforme se producen cambios en la tecnología de firma digital, en las plataformas utilizadas por la Autoridad Certificante o en sus procedimientos, la ANSES elabora programas de capacitación específicos para todo el personal afectado. Los mismos serán realizados, al menos una (1) vez al año, siendo evaluados y otorgándose certificación cuando así correspondiere. Los contenidos básicos se centrarán, entre otros, en los siguientes puntos relevantes:

- Infraestructura de firma digital.
- Responsabilidades y compromisos en roles y funciones.
- Procedimientos y políticas operacionales y de seguridad.
- Uso y operaciones de hardware y software empleado.
- Manejo de incidentes y compromisos en materia de seguridad.
- Procedimientos de recuperación ante desastres y manejo de la contingencia para la continuidad de actividades de la AC.
- Gestión de documentación inherente al funcionamiento de la AC.
- Simulacros sobre el sitio de contingencia, con una periodicidad de al menos dos veces al año.

5.3.4. - Frecuencia de rotación de cargos

No existe rotación entre los distintos cargos de la Autoridad Certificante.

5.3.5. - Sanciones a aplicar por acciones no autorizadas

De acuerdo a la Resolución D.E.A N° 93/93 aprobatoria del Reglamento de Personal y Régimen Disciplinario de ANSES, se establece en el artículo 15 del Capítulo V "La transgresión de las reglas fijadas en este Reglamento, legislación y normativa vigente y en el Convenio Colectivo aplicable, dará lugar a la aplicación de las sanciones disciplinarias que a continuación se establecen: apercibimiento, suspensión y despido.

Las sanciones se graduarán teniendo en cuenta la gravedad de las faltas, las circunstancias del caso, los antecedentes del empleado y la existencia de perjuicio."

Asimismo, cada tipo de sanción a aplicar se encuentra detallada en los artículos 16, 17 y 18 del Capítulo V de la mencionada Resolución.

5.3.6. - Requisitos para contratación de personal

J.G.M.
PRODESPA N°
3303

El personal a ser contratado a los efectos de cumplir acciones en el marco de esta Política de Certificación deberá poseer el conocimiento y formación suficiente, para el mejor cometido de las funciones asignadas. Para ello, la ANSES llevará a cabo los procesos de selección de personal y capacitación que estime necesarios con el objeto de que el perfil profesional del empleado se adecue lo más posible a las características propias de las tareas a desarrollar.

5.3.7. - Documentación y materiales provistos al personal

Todo el personal involucrado en el funcionamiento de la Autoridad Certificante es designado en sus funciones y comunicado de las tareas y procedimientos que debe cumplir.

Del mismo modo, si su función requiere de material adicional, como por ejemplo dispositivos criptográficos, cajas de seguridad, llaves, tarjetas de acceso, etc., éstos son entregados como paso previo a iniciar sus tareas.

En conformidad con el material entregado, el personal firma un acuse de recibo y compromiso de confidencialidad en los casos correspondientes.

6. - CONTROLES DE SEGURIDAD TECNICA

6.1. - Generación e instalación del par de claves criptográficas

6.1.1. - Generación del par de claves criptográficas

Las claves criptográficas de la Autoridad Certificante son generadas en ambientes seguros, por personal autorizado, sobre dispositivos criptográficos homologados FIPS 140-2 Nivel 3.

La Autoridad Certificante utiliza claves generadas mediante el algoritmo RSA con un tamaño de 4096 bits.

La clave criptográfica de la Autoridad de Registro es generada por su responsable utilizando un dispositivo criptográfico que cuenta con la certificación FIPS 140-2 Nivel 2.

La Autoridad de Registro genera su clave mediante el algoritmo RSA con un tamaño mínimo de 1024 bits.

Las claves criptográficas de los suscriptores son generadas y almacenadas en dispositivos criptográficos FIPS 140-2 Nivel 2.

Los suscriptores generan sus claves mediante el algoritmo RSA con un tamaño mínimo de 1024 bits.

6.1.2. - Entrega de la clave privada al suscriptor

Las claves privadas de los suscriptores son generadas por ellos mismos durante el proceso de solicitud, absteniéndose la ANSES de generar, exigir o por cualquier otro medio tomar conocimiento o acceder a sus datos de creación de firma.

Para la generación y almacenamiento de las claves los suscriptores cuentan con dispositivos criptográficos externos removibles que las protegen por medio de dos factores de seguridad: 1) mediante la posesión del dispositivo, 2) mediante un PIN o contraseña definida por el propio suscriptor

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

J.G.M. PRODESPA N° 3303

La clave pública del solicitante es entregada a la Autoridad Certificante durante el proceso de solicitud de certificado utilizando técnicas de "prueba de posesión" de la clave privada asociada.

Los procesos de solicitud utilizan el formato PKCS#10 para implementar la "prueba de posesión", remitiendo los datos del solicitante y su clave pública dentro de una estructura firmada con su clave privada.

Los solicitantes deben probar su identidad y demostrar que la solicitud les pertenece, presentándose frente a la Autoridad de Registro con un recibo de la solicitud en el cual se identifica la huella criptográfica de ésta.

6.1.4. - Disponibilidad de la clave pública del certificador

Los certificados de la "Autoridad Certificante para Personas Físicas de la ANSES" y el certificado de la "Autoridad Certificante Raíz de la República Argentina" (ACR RA) se encuentran disponibles en un repositorio en línea de acceso público a través de Internet.

La verificación de integridad de los certificados publicados puede realizarse cotejando sus firmas digitales a partir del certificado de la "Autoridad Certificante Raíz de la República Argentina" o corroborando las huellas criptográficas de éstos con las que fueran publicadas oportunamente en el Boletín Oficial de la Nación.

6.1.5. - Tamaño de claves

La AC de ANSES utiliza claves RSA con un tamaño de 4096 bits.

La Autoridad de Registro utiliza claves RSA con un tamaño mínimo de 1024 bits.

Los suscriptores de certificados utilizan claves RSA con un tamaño mínimo de 1024 bits.

6.1.6. - Generación de parámetros de claves asimétricas

No se establecen condiciones especiales para la generación de parámetros de claves asimétricas más allá de los que corresponden con el algoritmo de generación RSA según su especificación técnica.

6.1.7. - Verificación de calidad de los parámetros

No se requieren verificaciones particulares de la calidad de los parámetros de generación de claves.

6.1.8. - Generación de claves por hardware o software

Las claves de la Autoridad Certificante son generadas por hardware sobre dispositivos criptográficos FIPS 140-2 nivel 3.

Las claves de la Autoridad de Registro son generadas por hardware sobre dispositivos criptográficos FIPS 140-2 nivel 2.

Las claves de los suscriptores son generadas por hardware a través de dispositivos criptográficos que cumplen con las normas FIPS 140-2 nivel 2.

6.1.9. - Propósitos de utilización de claves (campo "KeyUsage" en certificados X.509 v.3)

Las claves criptográficas de los suscriptores podrán ser utilizadas para firma digital, respetando el alcance definido en la presente política de certificación. Los valores a utilizar son: "Firma Digital y Sin Repudio".

6.2. - Protección de la clave privada

La protección de la clave privada, considerada en este punto, se aplica para la Autoridad Certificante, la Autoridad de Registro y los suscriptores, según se detalla a continuación.

6.2.1. - Estándares para dispositivos criptográficos

La clave privada de la Autoridad Certificante es generada y almacenada sobre un dispositivo criptográfico diseñado para tal fin que cumple con las normas FIPS 140-2 nivel 3.

La clave privada de la Autoridad de Registro es generada y almacenada sobre un dispositivo criptográfico diseñado para tal fin que cumple con las normas FIPS 140-2 nivel 2.

La clave privada del suscriptor es generada y almacenada sobre dispositivos criptográficos diseñados para tal fin que cumplen con las normas FIPS 140-2 nivel 2.

6.2.2. - Control "M de N" de clave privada

La clave privada de la Autoridad Certificante es activada exclusivamente en las instalaciones de la ANSES o en su sitio de contingencia, dentro del nivel de seguridad (nivel de operaciones críticas de la Autoridad Certificante). Para su activación deben estar presentes, por lo menos, el responsable técnico, el oficial de seguridad y los oficiales habilitadores.

La Autoridad de Registro y los suscriptores de certificados tienen acceso a su clave privada contenida en su dispositivo criptográfico personal a través de un PIN o contraseña.

6.2.3. - Recuperación de clave privada

En caso de necesidad, la Autoridad Certificante prevé mecanismos de recuperación de sus claves privadas a partir de las copias de respaldo. Esta recuperación sólo puede ser realizada por personal autorizado, sobre uno de los dispositivos criptográficos seguros de los que

dispone la ANSES y exclusivamente en los niveles de seguridad de la Autoridad Certificante en su sitio principal o en su sitio de contingencia.

No se implementan mecanismos de resguardo y recuperación de la clave privada de la Autoridad de Registro, ni de los restantes suscriptores. En caso de compromiso de la clave privada, éstos deberán proceder a la revocación del certificado y tramitación de una nueva solicitud de emisión de certificado si así correspondiere.

6.2.4. - Copia de seguridad de clave privada

Copias de la clave privada de la Autoridad Certificante son realizadas inmediatamente después de su generación por personal autorizado y son almacenadas en dispositivos criptográficos seguros homologados FIPS 140-2 nivel 3.

No se implementa mecanismos de copias de resguardo de la clave privada de la Autoridad de Registro y de los suscriptores.

J.G.M. PRODESPA N° 3303

6.2.5. - Archivo de clave privada

Las copias de resguardo de la clave privada de la Autoridad Certificante son conservadas en lugares seguros, al igual que sus elementos de activación, bajo los niveles de seguridad previstos por la Decisión Administrativa N° 6/07.

No se implementa mecanismos de archivo de copias de resguardo de la clave privada de la Autoridad de Registro y de los suscriptores.

6.2.6. - Incorporación de claves privadas en dispositivos criptográficos

Las copias de resguardo de la clave privada de la Autoridad Certificante están soportadas en dispositivos criptográficos homologados FIPS 140-2 nivel 3.

La clave privada de la Autoridad de Registro y de los suscriptores es almacenada en el mismo dispositivo criptográfico donde es generada y no permite su exportación.

6.2.7. - Método de activación de claves privadas

Para la activación de la clave privada de la Autoridad Certificante deben estar presentes, por lo menos, el responsable técnico, el oficial de seguridad y los oficiales habilitadores. Los responsables necesarios para la activación deberán identificarse frente al sistema según corresponda al rol asignado por medio de distintos mecanismo de autenticación, a saber: llave de seguridad, claves secretas o ambos.

La Autoridad de Registro y los suscriptores tienen acceso a su clave privada y a su certificado contenidos en el dispositivo criptográfico a través de un PIN o contraseña.

6.2.8. - Método de desactivación de claves privadas

La desactivación de la clave privada de la Autoridad Certificante puede realizarse en forma automática o en forma manual.

La desactivación automática se produce en caso de apagado prolongado del dispositivo criptográfico que contiene esa clave privada.

La desactivación manual puede ser producida por el Responsable de Firma Digital previa identificación frente al sistema utilizando 2 factores de autenticación distintos: la posesión de una llave de seguridad más una clave secreta para habilitarla.

6.2.9. - Método de destrucción de claves privadas

Una vez finalizada la vida útil de la clave privada de la Autoridad Certificante, de la Autoridad de Registro y de los suscriptores, por motivo de revocación o expiración del certificado asociado, y de no mediar renovación del mismo, los dispositivos criptográficos serán formateados e inicializados nuevamente por la Gerencia de Seguridad Informática dependiente de la Gerencia de Sistemas y Telecomunicaciones de la ANSES.

6.3. - Otros aspectos de administración de claves

J.G.M. PRODESPA N° 3303

6.3.1. - Archivo permanente de la clave pública

Los certificados emitidos a suscriptores y a la Autoridad de Registro son almacenados y publicados bajo un esquema de redundancia y respaldados en forma periódica sobre dispositivos de sólo lectura, lo cual, sumado a la firma de los mismos, garantiza su integridad.

Todos los certificados son almacenados en soporte óptico y/o magnético, en formato estándar bajo codificación internacional DER. No se requieren herramientas particulares para el tratamiento de dicha información.

6.3.2. - Periodo de uso de clave pública y privada

Las claves privadas correspondientes a los certificados emitidos por la ANSES podrán ser utilizadas por su suscriptor únicamente durante el periodo de validez de los certificados, el cual tendrá una vigencia de 2 años. Las correspondientes claves públicas podrán ser utilizadas durante el periodo establecido por las normas legales vigentes, a fin de posibilitar la verificación de las firmas generadas durante su periodo de validez.

6.4. - Datos de activación

6.4.1. - Generación e instalación de datos de activación

Los dispositivos criptográficos utilizados por los suscriptores y la Autoridad de Registro para la generación, almacenamiento y uso de claves privadas son inicializados por personal de la Gerencia de Seguridad Informática dependiente de la Gerencia de Sistemas y Telecomunicaciones de la ANSES.

Como paso previo a la generación de claves, los suscriptores deberán establecer una clave de seguridad sobre el dispositivo denominado PIN o contraseña. Esta clave de seguridad, conocida sólo por el suscriptor, protege su clave privada e impide el acceso a la misma por parte de terceros, incluida la Autoridad Certificante.

6.4.2. - Protección de los datos de activación

Los suscriptores son responsables de la custodia de sus dispositivos criptográficos y de la no divulgación de sus claves, contraseñas y PIN de acceso.

La ANSES no implementa mecanismos de respaldo de las claves privadas de los suscriptores ni de sus datos de activación.

6.4.3. - Otros aspectos referidos a los datos de activación

Es responsabilidad de los suscriptores, elegir datos de activación para sus claves privadas que:

- Contengan como mínimo 8 símbolos, que incluyan letras mayúsculas, letras minúsculas y números.
- No sean fácilmente deducibles por otros (evitando utilizar nombres, direcciones, números telefónicos y similares relacionados con el suscriptor)

La contraseña de acceso al dispositivo criptográfico debe diferir de la clave de acceso a la clave privada.

6.5. - Controles de seguridad informática

6.5.1. - Requisitos Técnicos específicos

Para la prestación de sus servicios, la Autoridad Certificante para Personas Físicas de la ANSES utiliza una infraestructura tecnológica propia que cumple con los requisitos técnicos establecidos por la normativa vigente.

J.G.M. PRODESPA N° 3303

Entre los controles técnicos utilizados pueden mencionarse:

a) Control de Acceso físicos y lógicos

El acceso físico a las instalaciones está conformado por diversos perímetros de seguridad internos unos de otros, cada uno de los cuales cuenta con mecanismos de tarjeta de proximidad y/o biométricos.

Del mismo modo, el acceso lógico a los sistemas de *firewall* y sus propios mecanismos de control y monitoreo.

b) Separación de funciones y roles críticos

Las principales funciones vinculadas a los procesos de seguridad y certificación se encuentran divididos en roles que aseguran el correcto desempeño de los responsables designados.

Los roles definidos en la operatoria de la Autoridad Certificante serán desempeñados por diferentes responsables. Ninguno de los nombrados cumplirá más de una función o rol, ni aún cuando fuera en forma transitoria. En caso de ausencia temporaria, el responsable será reemplazado por su correspondiente sustituto.

c) Identificación y autenticación de roles

Para la identificación y autenticación en cada uno de los roles críticos vinculados al proceso de certificación y gestión de claves de la ANSES se utilizan mecanismos de reconocimiento biométrico y sistemas de autenticación de múltiples factores.

d) Utilización de criptografía para las sesiones de comunicación.

Todas las comunicaciones críticas entre los distintos componentes de la Autoridad Certificante se realizan en forma cifrada.

e) Archivo de datos históricos y de auditoría del certificador y usuarios

Se realizan auditorías y controles periódicos sobre cada etapa del proceso de certificación, incluyendo la verificación de la documentación de respaldo del proceso de identificación de suscriptores.

f) Registro de eventos de seguridad

Todas las operaciones y actividades de la ANSES generan información de control y registros de eventos que permiten verificar el funcionamiento y la seguridad de los sistemas.

g) Prueba de seguridad.

Se realizan comprobaciones periódicas del funcionamiento de los sistemas y los planes de contingencia.

h) Mecanismos de recuperación para claves y sistema de certificación.

Existen mecanismos y procedimientos de contingencia que garantizan la correcta prestación de los servicios.

J.G.M.
PRODESPA Nº
3303
7

6.5.2. - Calificaciones de seguridad computacional

La Autoridad Certificante para Personas Físicas de la ANSES se encuentra alojada dentro de una Sala Cofre del Centro de Procesamiento del Organismo, contando con las siguientes certificaciones:

a) Euronorma EN 1.047/2 Consejo Europeo de Certificación de Sistemas de Seguridad

b) Estanqueidad contra gases corrosivos en relación al agua de basamento y polvo según norma DIN 18.095

c) Testeada y probada en una situación real de incendio según Euronorma EN 1.047/2 y la norma VDMA Alemana 24.991/2

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

6.6.1. - Controles de desarrollo de sistemas

ANSES posee procedimientos específicos para el diseño y desarrollo de sistemas entre los cuales se encuentran:

a) metodologías estándar de análisis, especificación y diseño.

b) control de versiones de cada uno de los módulos y componentes desarrollados.

c) separación de ambientes de desarrollo, prueba y producción

6.6.2. - Administración de controles y seguridad

Se utilizan técnicas de sistemas de detección de intrusiones basadas en servidores (HIDS *Host Intrusion Detection System*) para identificar cualquier alteración no esperada en los sistemas o archivos de configuración.

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

No existen certificaciones de terceros respecto del ciclo de vida del software.

6.7. - Controles de seguridad de red

La red de la Autoridad Certificante se encuentra delimitada por diversos *firewalls* y monitoreada por un sistema de detección de intrusiones (IDS).

6.8. - Controles de ingeniería de dispositivos criptográficos

Todas las actualizaciones de software o firmware de los dispositivos criptográficos utilizados por la Autoridad Certificante, la Autoridad de Registro o los suscriptores son verificadas en ambientes de prueba independientes y, en caso de ser aprobados por el personal técnico de la ANSES, son distribuidos y aplicados en los sistemas correspondientes.

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

Todos los certificados emitidos bajo la presente Política de Certificación respetan la especificación ITU-T X.509 (ISO/IEC 9594-8) "*Information Technology – The Directory: Public key and atribute certificate frameworks*" adoptada como estándar tecnológico para la Infraestructura de Firma Digital de la República Argentina por la Decisión Administrativa 6/2007 de la JGM.

J.G.M. PRODESPA N° 3303 87

7.1. - Perfil del certificado

El formato de los certificados digitales emitidos bajo esta política cumple con los requerimientos de la Decisión Administrativa 6/2007 de la JGM y las especificaciones contenidas en RFC 3739 "*Internet X.509 Public Key Infrastructure Qualified Certificates Profile*" y RFC 3280 "*Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile*".

Campo	Valor	
Version	2	
serialNumber	Número de serie del certificado	
Signature	*<algoritmo de firma>* 1.2.840.113549.1.1.5 (SHA1-RSA)	
Issuer	<Nombre distintivo del emisor>	
– *commonName*	*2.5.4.3*	Autoridad Certificante para Personas Físicas de la ANSES
– *serialNumber*	*2.5.4.5*	CUIT 33637617449
– *description*	*2.5.4.13*	Certificador Licenciado - Ley 25506
– *organizationName*	*2.5.4.10*	Administración Nacional de la Seguridad Social
– *stateOrProvinceName*	*2.5.4.8*	Ciudad Autónoma de Buenos Aires
– *countryName*	*2.5.4.6*	AR
Validity	*<Validez (desde, hasta)>*	
– *notBefore*	*<fecha de emisión>*	
– *notAfter*	*<fecha de emisión* + 2 años>	

Subject	*<Nombre distintivo del suscriptor>*	
– *commonName*	*2.5.4.3*	*<Nombres y Apellidos>*
– *serialNumber*	*2.5.4.5*	CUIL *<11 dígitos del número de CUIL sin guiones>*
– *description*	*2.5.4.13*	userID *<identificación de usuario de red>*
– *emailAdrress*	*1.2.840.113549.1.9.1*	*<dirección de correo electrónico>*
– *title*	*2.5.4.12*	*<cargo o función que desempeña>*
– *organizationalUnitName*	*2.5.4.11*	*<área en la que ejerce el cargo o función>*
– *organizationName*	*2.5.4.10*	Administración Nacional de la Seguridad Social
– *stateOrProvinceName*	*2.5.4.8*	*<Ciudad en la que trabaja>*
– *localityName*	*2.5.4.7*	*<Provincia en la que trabaja>*
– *countryName*	*2.5.4.6*	AR
subjectPublicKeyInfo	*<clave pública del suscriptor>*	
extensions	***<Extensiones del certificado>***	
– *authorityKeyIdentifier*	*2.5.29.35*	*<identificador de la clave de la Autoridad Certificante para Personas Físicas de la ANSES>*
– *basicConstraint*	*2.5.29.19*	Tipo de suscriptor = Entidad Final, Restricción de logitud de ruta = 0
– *keyUsage*	*2.5.29.15*	*<usos de claves>* Firma digital, No-repudio
– *CRLDistributionPoints*	*2.5.29.31*	[1]CRL Distribution Point Distribution Point Name: Full Name: URL=https://*<servidor>/<path>/<archivoCRL.crl>* [2]CRL Distribution Point Distribution Point Name: Full Name: URL= http://*<srv.alternativo>/<path>/<archivoCRL.crl>* [3]CRL Distribution Point Distribution Point Name: Full Name: URL= ldap:///CN=*<servidor>*,CN=*<servidor>*,CN=CDP,CN=Public%20Key%20Services,CN=Services,CN=Configuration,DC=anses,DC=gov,DC=ar?certificateRevocationList?base?objectclass=cRLDistributionPoint
– *CertificatePolicies*	*2.5.29.32*	Política de Certificación: <Identificador de la Política> *<OID de politica, asignado por la Autoridad de Aplicación>* <Puntero al documento que contiene esta Política>

J.G.M.
PRODESPA Nº
3303

		http://<servidor>/<path>/<política.pdf> <Aviso para el usuario> <Certificado emitido por ANSES en el marco de la ley 25506>

7.2. - Perfil de la lista de certificados revocados

Las listas de certificados revocados (CRLs) cumplen con los requerimientos de la DA 6/2007 y las especificaciones contenidas en el RFC 3280 "*Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile*".

Campo	Valor	
Version	1	
Signature	*<algoritmo de firma>* 1.2.840.113549.1.1.5 (SHA1-RSA)	
Issuer	<Nombre distintivo del emisor>	
– *commonName*	*2.5.4.3*	Autoridad Certificante para Personas Físicas de la ANSES
– *serialNumber*	*2.5.4.5*	CUIT 33637617449
– *description*	*2.5.4.13*	Certificador Licenciado - Ley 25506
– *organizationName*	*2.5.4.10*	Administración Nacional de la Seguridad Social
– *stateOrProvinceName*	*2.5.4.8*	Ciudad Autónoma de Buenos Aires
– *countryName*	*2.5.4.6*	AR
thisUpdate	*<fecha y hora de emisión>*	
nextUpdate	*<fecha de próxima emisión>*	
revokedCertificates	**<Certificados Revocados>**	
– *serialNumber*	*<número de serie del certificado revocado>*	
– *revocationDate*	*<fecha de revocación>*	
– *ReasonCode*	*2.5.29.21*	*<Código de motivo de revocación >*
extensions	**<Extensiones de la CRL>**	
– *authorityKeyIdentifier*	*2.5.29.35*	*<identificador de la clave de la Autoridad Certificante para Personas Físicas de la ANSES>*
– *CRLNumber*	*2.5.29.20*	*<Nro. de secuencia de esta CRL>*

J.G.M. PRODESPA Nº 3303 7 865

8. - ADMINISTRACION DE ESPECIFICACIONES

8.1. - Procedimientos de cambio de especificaciones

El presente documento será revisado y actualizado en forma periódica por la ANSES y puesto en vigencia, previa aprobación de la Autoridad de Aplicación.

Las nuevas versiones de la política contendrán una referencia a cada una de las versiones previas, junto a una descripción sintética de los principales cambios introducidos.

8.2. - Procedimientos de publicación y notificación

Una copia actualizada del presente documento se encuentra disponible en forma pública y accesible a través de Internet en la dirección:

https://servicioswww.anses.gov.ar/firmadigital/

En caso de producirse modificaciones sustanciales a los contenidos de la presente política, los suscriptores que posean certificados vigentes a la fecha de aplicación del cambio serán notificados por correo electrónico en las direcciones declaradas en los correspondientes certificados.

8.3. - Procedimientos de aprobación

Según los establecido por la Ley 25.506 Art. 21 inc. q) y por la Decisión Administrativa 6/2007 la presente política y sus modificaciones deben ser aprobadas por la Autoridad de Aplicación.

J.G.M.
PRODESPA Nº
3303