Jefatura de Gabinete de Ministros
Secretaría de Gabinete y Coordinación Administrativa

327

COORDINACIÓN DE DESPACHO Y PROTOCOLIZACIÓN
FOLIO
Nº 106
J.G.M.

BUENOS AIRES, 6 AGO 2013

VISTO el Expediente N° CUDAP:JGM:0024658/2013 del registro de la JEFATURA DE GABINETE DE MINISTROS, la Ley N° 25.506, los Decretos N° 2.628 del 19 de diciembre de 2002 y sus modificatorios y N° 22 del 10 de diciembre de 2011, la Decisión Administrativa N° 6 del 7 de febrero de 2007, las Resoluciones N° 63 del 13 de noviembre de 2007 de la ex SUBSECRETARÍA DE LA GESTIÓN PÚBLICA de la JEFATURA DE GABINETE DE MINISTROS y N° 184 del 28 de junio de 2012 de la SECRETARÍA DE GABINETE Y COORDINACIÓN ADMINISTRATIVA de la JEFATURA DE GABINETE DE MINISTROS, y

CONSIDERANDO:

Que la Ley N° 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.

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.

J. G. M.
FOLIO
2119

Que el artículo 24 del Decreto N° 2.628 del 19 de diciembre de 2002 y sus modificatorios, reglamentario de la Ley N° 25.506, establece el procedimiento que los certificadores deben observar para la obtención de una licencia y detalla la documentación exigida para el cumplimiento de las condiciones estipuladas en la Ley N° 25.506, su decreto reglamentario y normas complementarias.

Que la Decisión Administrativa N° 6 del 7 de febrero de 2007 establece las pautas 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 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 la mencionada Decisión Administrativa prescribe en su artículo 26 que los certificadores licenciados están obligados a notificar al ente licenciante cualquier modificación que proyecten realizar sobre los aspectos que fueron objeto de revisión para el otorgamiento de su licencia, reservándose el ente licenciante la facultad de aceptar o rechazar dichos cambios.

Jefatura de Gabinete de Ministros
Secretaría de Gabinete y Coordinación Administrativa

327

COORDINACIÓN DE DESPACHO Y PROTOCOLIZACIÓN FOLIO Nº 107 J.G.M.

Que la Resolución de la ex SUBSECRETARÍA DE LA GESTIÓN PÚBLICA de la JEFATURA DE GABINETE DE MINISTROS N° 63 del 13 de noviembre de 2007 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 TENOLOGÍAS DE INFORMACIÓN de la SUBSECRETARÍA DE TECNOLOGÍAS DE GESTIÓN de la SECRETARÍA DE GABINETE Y COORDINACIÓN ADMINISTRATIVA de la JEFATURA DE GABINETE DE MINISTROS, la facultad de asignar el número de identificador de objeto –OID- a la política de certificación licenciada, de acúerdo a lo previsto en el inciso 1.2 del Anexo de la mencionada Resolución.

Que el Decreto N° 22 del 10 de diciembre de 2011 en el punto 35 de la Planilla Anexa al artículo 2°, faculta a la SECRETARÍA DE GABINETE Y COORDINACIÓN ADMINISTRATIVA de la JEFATURA DE GABINETE DE MINISTROS a entender en el régimen normativo de la Infraestructura de Firma Digital establecido por la Ley N° 25.506, y en las funciones de ente licenciante y supervisor de certificadores.

J. G. M. PROY. 119

Que la Resolución de la SECRETARÍA DE GABINETE Y COORDINACIÓN ADMINISTRATIVA de la JEFATURA DE GABINETE DE MINISTROS N° 184 del 28 de junio de 2012 aprobó la "Política de Certificación para Personas Físicas y Jurídicas de ENCODE S.A." presentada por dicha firma, a la cual otorgó en dicho acto una licencia para operar como certificador licenciado en el marco de la Infraestructura de Firma Digital creada por Ley N° 25.506.

Que la mencionada firma presentó una nueva versión de la Política de Certificación citada, solicitando la consideración por parte del ente licenciante de varias modificaciones respecto al texto original.

Que una de las modificaciones solicitadas consistía en la inclusión de autorizados, apoderados, afiliados, matriculados o inscriptos de las personas físicas o jurídicas de naturaleza pública o privada, entre los posibles suscriptores de certificados digitales emitidos por la Autoridad Certificante correspondiente a la Política de Certificación aprobada.

Que, adicionalmente, se solicitaba el agregado de otros convenios por locaciones de servicios en el listado que originalmente describía el marco normativo aplicable a la emisión de certificados digitales por parte del certificador licenciado.

Jefatura de Gabinete de Ministros
Secretaría de Gabinete y Coordinación Administrativa

327

FOLIO Nº 108

Que, asimismo, se requería la modificación del apartado d) del listado de aplicaciones para las cuales son pasibles de utilización los certificados digitales emitidos bajo la Política de Certificación aprobada, agregándose también los documentos electrónicos firmados digitalmente que se intercambien y/o presenten entre las distintas organizaciones o entidades con los suscriptores de certificados o entre dichos suscriptores, en el marco de normas aplicables a la comunidad de suscriptores y de aplicaciones.

Que analizadas dichas modificaciones por la OFICINA NACIONAL DE TECNOLOGÍAS DE INFORMACIÓN de la SUBSECRETARÍA DE TECNOLOGÍAS DE GESTIÓN de la SECRETARÍA DE GABINETE Y COORDINACIÓN ADMINISTRATIVA de la JEFATURA DE GABINETE DE MINISTROS, dicha instancia no encontró observaciones que formular.

Que se ha cumplido con todos los recaudos procedimentales establecidos en la normativa, según consta en el Expediente N° 39448/11 y sus agregados citados en el Visto de la presente medida.

Que la SUBSECRETARÍA DE TECNOLOGÍAS DE GESTIÓN de la SECRETARÍA DE GABINETE Y COORDINACIÓN ADMINISTRATIVA de la JEFATURA DE GABINETE DE MINISTROS ha tomado la intervención que le compete.

J. G. M. PROY.

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

Que la presente medida se dicta en virtud de las facultades conferidas por el Decreto N° 357 del 21 de febrero de 2002 y sus modificatorios.

Por ello,

EL SECRETARIO DE GABINETE Y COORDINACIÓN ADMINISTRATIVA
DE LA JEFATURA DE GABINETE DE MINISTROS
RESUELVE:

ARTÍCULO 1°.- Apruébase la nueva versión de la "Política de Certificación para Personas Físicas y Jurídicas de ENCODE S.A.", que como Anexo forma parte integrante de la presente, bajo la cual el certificador licenciado deberá emitir certificados digitales a partir de la publicación de la presente.

Jefatura de Gabinete de Ministros
Secretaría de Gabinete y Coordinación Administrativa

COORDINACIÓN DE DESPACHO Y PROTOCOLIZACIÓN
FOLIO
Nº 109

ARTÍCULO 2°.- Instrúyese a la OFICINA NACIONAL DE TECNOLOGÍAS DE INFORMACIÓN de la SUBSECRETARÍA DE TECNOLOGÍAS DE GESTIÓN de la SECRETARÍA DE GABINETE Y COORDINACIÓN ADMINISTRATIVA de la JEFATURA DE GABINETE DE MINISTROS, conforme Resolución de la SUBSECRETARÍA DE LA GESTIÓN PÚBLICA de la JEFATURA DE GABINETE DE MINISTROS N° 63 del 13 de noviembre de 2007, 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 por la presente.

ARTÍCULO 3°.- Autorízase la divulgación de la nueva versión de la Política de Certificación en el sitio de publicación de la Autoridad Certificante Raíz de la República Argentina.

ARTÍCULO 4°.- Comuníquese, publíquese, dese a la Dirección Nacional del Registro Oficial y archívese.

RESOLUCIÓN SGCA N° 327

Lic. FACUNDO P. NEJAMKIS
Secretario de Gabinete
y Coordinación Administrativa
Jefatura de Gabinete de Ministros

J. G. M.
FOLIO
2119

327

ANEXO

ENCODE S.A.

POLÍTICA DE CERTIFICACIÓN
PARA PERSONAS FÍSICAS Y JURÍDICAS
DE ENCODE S. A.

POLÍTICA DE CERTIFICACIÓN

VERSIÓN 1.8

Versiones y modificaciones de este documento

V	M	Fecha	Elaborado por	Revisado por	Descripción
1	0	2010-07-16	GrupoFD	Directorio ENCODE	Aprobación para presentación
1	1	2010-12-16	GrupoFD	Directorio ENCODE	Aprobación modificaciones
1	2	2011-06-24	GrupoFD	Directorio ENCODE	Aprobación modificaciones
1	3	2011-08-18	GrupoFD	Directorio ENCODE	Clase de Certificado, Puesto de Atención, Suscriptor, Aranceles, Correo Electrónico, CommonName, SubjetAlternativeName, Escribano, Segundo Control, Aceptación del Certificado, Aplicaciones habilitadas, FIPS, OWASP y Legislación
1	4	2011-09-26	GrupoFD	Directorio ENCODE	Aprobación modificaciones
1	5	2011-11-01	GrupoFD	Directorio ENCODE	Aprobación modificaciones
1	6	2012-11-01	GrupoFD	Directorio ENCODE	Aprobación modificaciones
1	7	03-04-2013	GrupoFD	Directorio ENCODE	Aprobación modificaciones
1	8	29-04-2013	GrupoFD	Directorio ENCODE	Aprobación modificaciones

J. C. M. PROY. 2119

INDICE

1. - INTRODUCCIÓN

1.1. – Descripción general

El presente documento es la Política de Certificación de ENCODE S. A. para Personas Físicas y Jurídicas (en adelante "Política de Certificación") OID 2.16.32.1.1.4 de conformidad con la Ley Nº 25.506, su Decreto Reglamentario Nº 2628/2002 y la Decisión Administrativa Nº 6/2007 de la Jefatura de Gabinete de Ministros, Política Licenciada mediante resolución 184/2012 de la Secretaría de Gabinete y Coordinación Administrativa.

En esta Política se establecen las responsabilidades de:

- ENCODE S. A. como Certificador Licenciado,
- AC ENCODESIN como Autoridad Certificante
- la Autoridad de Registro Central y las Autoridades de Registro Delegadas,
- 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 comprende la emisión de certificados digitales a personas físicas y jurídicas, autorizando el uso de los certificados emitidos de acuerdo con lo establecido en el apartado "1.3.4 – Aplicabilidad".

1.2. – Identificación

Nombre:	Política de Certificación de ENCODE S. A. para Personas Físicas y Jurídicas
Versión:	1.8
Fecha:	[completar luego de su aprobación por parte de la Autoridad de Aplicación]
URL:	http://www.encodeac.com.ar/firma-digital/ENCODESIN.pdf
OID:	2.16.32.1.1.4
Lugar:	República Argentina

1.3. - Participantes y aplicabilidad

1.3.1. - Certificador

ENCODE S.A. en su calidad de Certificador Licenciado, con licencia otorgada por Resolución Nº 184 de la Secretaría de Gabinete y Coordinación Administrativa en su carácter de Autoridad de Aplicación de la Infraestructura de Firma Digital de la República Argentina (IFDRA), presta los servicios de certificación digital según lo establecido por la Ley 25.506 y sus normas complementarias. Presenta esta nueva versión de la política Licenciada cuyo OID es 2.16.32.1.1.4, de acuerdo a los establecido en artículo 21 de la ley 25506.-y articulo 26 de la Decisión Administrativa 06/2007.-

A los fines de desarrollar las referidas tareas se constituye la Autoridad Certificante ENCODESIN de ENCODE S.A. para Personas Físicas y Jurídicas, en adelante "Autoridad Certificante" o "AC ENCODESIN".

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 las Autoridades de Registro. Existe una Autoridad de Registro Central, operada por ENCODE S.A., en todo el territorio argentino y Autoridades de Registro Delegadas, las que son operadas por Organizaciones que, a dichos efectos, hayan convenido con ENCODE S.A. Estas autoridades de registro delegadas están bajo el control y supervisión de la Autoridad de Registro Central de ENCODE S.A.

Las Autoridades de Registro habilitadas se publicarán en el sitio:

- http://www.encodeac.com.ar/autoridades-de-registro.html

La información relacionada con las Organizaciones que adopten la utilización de certificados digitales emitidos por la AC de ENCODE S.A., en los términos de esta Política de Certificación, se publicará en el sitio:

- http://www.encodeac.com.ar/firma-digital/organizaciones.html

1.3.3. - Suscriptores de certificados

Según los términos de la presente política de certificación, podrán ser suscriptores de certificados digitales Las personas físicas o jurídicas de naturaleza Pública o Privada, sus respectivos empleados, autorizados, apoderados, afiliados, matriculados, o inscriptos, quienes en cumplimiento de sus obligaciones deban intercambiar y/o presentar ante quien corresponda documentación exigida por la normativa vigente, por medio de aplicaciones, registros procedimientos y trámites que soportan la utilización de los certificados emitidos por la AC ENCODESIN de ENCODE SA conforme al marco normativo especificado en 1.3.4. Aplicabilidad.-

Los certificados digitales emitidos bajo la presente política son expedidos a favor de personas físicas y de personas jurídicas públicas o privadas a título oneroso, aplicándose aranceles diferenciales conforme al tipo de certificado que se expida.

Existen varias clases para cada tipo de certificado según las condiciones del Suscriptor.

Certificados de clase A para persona física empleador

Son aquellos emitidos a favor de un empleador persona física que suministran confianza respecto a la identidad del suscriptor.

Certificado de clase A para persona jurídica, empleador

Son emitidos a favor de una persona jurídica pública o privada empleador solicitados por su representante legal debidamente autorizado o bien por su apoderado autorizado con poder general amplio o especial al efecto, a los fines que se emplee el certificado en representación de la persona jurídica.

Certificados de clase B para persona física

Son emitidos a favor de una persona física en relación de dependencia con el titular de un certificado de clase A, al momento de la solicitud del certificado clase B. El sistema enviará la solicitud de certificado clase B al titular del certificado clase A relacionado, a los fines de que este último autorice la solicitud con su certificado.

Certificados de clase C para persona física

Son emitidos a favor de una persona física que no se encuentre en relación de dependencia con el titular de un certificado de clase A, sino vinculado a este a través de un contrato de locación de servicios, o como afiliado, o matriculado, o inscripto al momento de la solicitud del certificado clase C. El sistema enviará la solicitud de certificado clase C al titular del certificado clase A relacionado, a los fines de que este último autorice la solicitud con su certificado.

El titular del certificado clase A relacionado con el certificado de clase B o C se hará responsable a los efectos de la utilización de estos últimos, según los alcances especificados en la nota de autorización generada al momento de la solicitud del certificado clase B o C y firmada por el titular del certificado clase A, no asumiendo ENCODE S.A. responsabilidad alguna a dichos fines o efectos.

Asignación de clases de certificados

La aplicación del Certificador, en base a la información confirmada por el Solicitante, determina y asigna automáticamente la clase y el tipo de los certificados enunciados

precedentemente una vez iniciado el proceso de solicitud de certificado digital con el siguiente criterio:

Certificado de clase A: Cuando se trate de una persona física o jurídica pública o privada empleador al momento de suscripción del certificado. La vigencia de este certificado será de un (1) año.

Certificado de clase B: Cuando se trate de una persona física en relación de dependencia con el titular del certificado clase A, al momento de suscripción del certificado. La vigencia de este certificado será de un (1) año.

Certificado de clase C: Cuando se trate de una persona física sin relación de dependencia con el titular del certificado clase A, sino vinculado a este a través de un contrato de locación de servicios o como afiliado, matriculado, o inscripto, al momento de la solicitud del certificado clase C. -. La vigencia de este certificado será de un (1) año.

J. G. M. PROY. 2119

1.3.4. - Aplicabilidad

Los certificados emitidos por la Autoridad Certificante ENCODESIN de ENCODE S.A. se podrán utilizar en el marco del cumplimiento de las obligaciones o relaciones descriptas en el punto 1.3.3.- Suscriptores, de la presente Política de Certificación.

Los certificados digitales emitidos en el marco de la presente Política de Certificación podrán ser utilizados exclusivamente en las aplicaciones que se encuentran detalladas a continuación:

a) Documentos de carácter laboral exigidos por la normativa vigente presentada ante asociaciones sindicales, firmados digitalmente que se intercambien entre las personas físicas y/o jurídicas suscriptores de certificados y las organizaciones sindicales.

b) Documentos de carácter laboral exigidos por la normativa vigente presentada ante distintos organismos laborales públicos con competencia en el ámbito nacional y provincial, firmados digitalmente que se intercambien entre las personas físicas o jurídicas suscriptores de certificados y dichos organismos laborales públicos.

c) Documentos de carácter laboral exigidos por la normativa vigente, firmados digitalmente que se intercambien entre las personas físicas o jurídicas suscriptores de certificados y/o sus empleados.

d) Declaraciones juradas autodeterminativas de aportes y/o contribuciones, o documentos electrónicos firmados digitalmente que se intercambien y/o presenten entre las distintas organizaciones o entidades profesionales con los suscriptores de certificados o entre dichos suscriptores, en el marco de normas aplicables a la comunidad de suscriptores y de aplicaciones.

e) Presentaciones de documentación exigidas por los convenios colectivos de trabajo de las entidades sindicales a las que pertenecen dicho convenios firmados digitalmente que

se intercambien entre las personas físicas y/o jurídicas suscriptores de certificados y las organizaciones sindicales .-

Marco normativo aplicable a la comunidad de suscriptores y de aplicaciones:

ENCODE S.A. deja expresado que el marco de aplicación de la presente Política de su Autoridad Certificante ENCODESIN, definida en los puntos 1.3.3.- Suscriptores de certificados y 1.3.4.- Aplicabilidad, no invade ni interfiere el ámbito de competencia que la legislación vigente le otorga expresamente a la Administración Federal de Ingresos Públicos (AFIP).

El marco normativo legal vigente aplicable a la presente Política de Certificación, además de las normas específicas que regulan los servicios de Firma Digital, está conformado por:

- Ley de Convenciones Colectivas de Trabajo
- Ley de asociaciones sindicales o de entidades que nuclean profesionales
- Ley de aportes y contribuciones a entidades gremiales
- Ley de contrato de trabajo
- Ley de Obras sociales
- Ley sobre Recursos y procedimientos de la Seguridad Social
- Leyes de fondos provinciales, y toda otra legislación Provincial que reglamente la fiscalización control y habilitación de la documentación con competencia propia de cada provincia exigida entre otras por la legislación laboral, previsional, de la seguridad social e Impositiva.-
- Convenios Colectivos de Trabajo comprensivos de las distintas actividades llevadas a cabo por los suscriptores de la presente política.
- Otros convenios por locaciones de servicios no comprendido en el párrafo anterior

1.4. - Contactos

Esta Política de Certificación es administrada por ENCODE S. A.:

Contacto: Responsable de la Autoridad de Registro Central

Domicilio: Arturo M. Bas 34 Local PB - X5000KLB – Córdoba – Provincia de Córdoba

E-mail: arc@encodesa.com.ar

Teléfono: 54 (351) 569-4407 o 569-4408 y líneas rotativas

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

Contacto: Responsable Mesa de Ayuda

Domicilio: Arturo M. Bas 34 Local PB - X5000KLB – Córdoba – Provincia de Córdoba

E-mail: mda@encodesa.com.ar

Teléfono: 54 (351) 569 4407 o 569 4408 y líneas rotativas

2. - ASPECTOS GENERALES DE LA POLÍTICA DE CERTIFICACION

2.1. - Obligaciones

2.1.1. - Obligaciones del Certificador

Son obligaciones de ENCODE S. A. en su carácter de Certificador Licenciado:

Ley Nº 25.506, artículo 21 -

ENCODE S. A. en su carácter de Certificador Licenciado cumplirá con:

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

b) Abstenerse de generar, exigir, o por cualquier otro medio tomar conocimiento o acceder bajo ninguna circunstancia, a los datos de

creación de firma digital de los titulares de certificados digitales por él emitidos;

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

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

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

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

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

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

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

j) Incorporar en su Política de Certificación los efectos de la revocación de su propio certificado y/o de la licencia que le otorgara la Autoridad de Aplicación;

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

l) Publicar en el Boletín Oficial aquellos datos que la Autoridad de Aplicación determine;

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

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

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

p) Solicitar inmediatamente 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;

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

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

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

t) Someter a aprobación de la Autoridad de Aplicación el manual de procedimientos, el plan de seguridad y el de cese de actividades, así como el detalle de los componentes técnicos a utilizar;

u) Constituir domicilio legal en la República Argentina;

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

w) Cumplir con toda otra obligación emergente de su calidad de titular de la licencia adjudicada por el ente licenciante.

J. G. M. PROY.

2119

Decreto Nº 2628/02, artículos 34 y 36

ENCODE S. A. en su carácter de Certificador Licenciado cumplirá con:

a) Comprobar por sí o por medio de una Autoridad de Registro que actúe en nombre y por cuenta suya, la identidad y cualquier otro dato de los solicitantes considerado relevante para los

procedimientos de verificación de identidad previos a la emisión del certificado, según la Política de Certificación bajo la cual se solicita.

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

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

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

e) Informar al solicitante de un certificado, 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 servicios asociados, incluyendo cargos adicionales y formas de pago, los niveles de servicio a proveer, las obligaciones que el suscriptor asume como usuario del servicio de certificación, su domicilio en la República Argentina y los medios a los que el suscriptor puede acudir para solicitar aclaraciones, dar cuenta del mal funcionamiento del sistema o presentar sus reclamos.

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

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

h) Mantener actualizados los repositorios de certificados revocados por el período establecido por la Autoridad de Aplicación.

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

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

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

J. G. M.
PROY.
2119

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

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

n) Revocar los certificados digitales por él emitidos en los casos enumerados en el punto e) del artículo 19 de la Ley Nº 25.506.

En caso de ocurrir el supuesto enumerado en el punto 3 del inciso e) del artículo 19 se deberá sustituir en forma gratuita aquel certificado que ha dejado de ser seguro por otro que sí cumpla con ese requisito.

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.

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

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

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

r) 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 las Autoridades de Registro las indemnizaciones por los daños y perjuicios que aquél sufriera como consecuencia de los actos y/u omisiones de éstas.

Obligaciones adicionales y aclaraciones

ENCODE S. A. en su carácter de Certificador Licenciado cumplirá también con:

a) Notificar a sus suscriptores sobre cualquier acontecimiento que pudiera ocasionar el compromiso de su clave privada y la generación de un nuevo par de claves.

b) Notificar a sus suscriptores y a la Autoridad de Aplicación acerca del cese de sus actividades.

c) Emitir y distribuir los certificados a sus suscriptores, informándolos acerca de dicha emisión.

d) Cumplir con todas y cada una de las obligaciones establecidas en la Decisión Administrativa Nº 6/2007 y sus Anexos.

e) Cumplir con todas las medidas de seguridad establecidas en su Política de Seguridad.

f) Sustituir en forma gratuita los certificados de suscriptores que hubieran sido revocados por haberse determinado que los procedimientos de emisión y/o verificación han dejado de ser seguros, de acuerdo con lo previsto en la ley 25506, artículo 19, inciso e), apartado 3.

En esos casos el suscriptor deberá solicitar el reemplazo de su certificado digital de acuerdo con el procedimiento que determine ENCODE S.A.

Si un certificado digital hubiera dejado de ser seguro por razones atribuibles a su titular, ENCODE S.A. no estará obligada a entregar un nuevo certificado digital.

2.1.2. - Obligaciones de la Autoridad de Registro

Son obligaciones de la Autoridad de Registro:

Decreto Nº 2628/02, artículos 35

Las Autoridades de Registro cumplirán con:

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

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

c) La validación de otros datos de los titulares de certificados que se presenten ante ellas, cuya verificación delegue ENCODE S.A.

d) La remisión de las solicitudes aprobadas a la Autoridad Certificante ENCODESIN.

e) La recepción y validación de las solicitudes de revocación de certificados; y su direccionamiento a la Autoridad Certificante ENCODESIN.

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

g) El archivo y la conservación de toda la documentación de respaldo del proceso de validación de identidad, de acuerdo con los procedimientos establecidos por ENCODE S.A.

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

i) El cumplimiento de las disposiciones que establece esta Política de Certificación y su Manual de Procedimientos, en la parte que resulte aplicable.

Obligaciones adicionales y aclaraciones

Las Autoridades de Registro cumplirán también con:

a) Las normas y recaudos establecidos para la protección de claves privadas y de seguridad física y lógica, entre los que se incluye la protección de sus propias claves privadas.

b) Todas las medidas de seguridad establecidas por ENCODE S.A. en el documento titulado "Guía de instalación y funcionamiento de las Autoridades de Registro".

2.1.3. - Obligaciones de los Suscriptores de los certificados

Son obligaciones de los suscriptores de certificados cumplir con:

Ley Nº 25.506, artículo 25

Los Suscriptores de certificados deberán:

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

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

c) Solicitar la revocación de su certificado al Certificador Licenciado ENCODE S.A., ante cualquier circunstancia que pueda haber comprometido la privacidad de sus datos de creación de firma;

d) Informar sin demora al certificador licenciado ENCODE S.A., el cambio de alguno de los datos contenidos en el certificado, oportunamente suministrados por el suscriptor, y que hubiera sido objeto de verificación.

Obligaciones adicionales

Los Suscriptores de certificados deberán también:

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

b) Utilizar sus certificados de forma adecuada, conforme a lo previsto en esta Política de Certificación.

c) Tomar conocimiento de los derechos y obligaciones que se establecen en esta Política de Certificación, en el Manual de Procedimientos de Certificación (en sus aspectos no confidenciales), en el Acuerdo con Suscriptores y en todo documento aplicable.

d) Solicitar la revocación de su certificado en caso de ocurrir algún cambio que lo excluya de la aplicación de la presente política.

2.1.4. - Obligaciones de los terceros usuarios

Decisión Administrativa Nº 06/2007 de la Jefatura de Gabinete de Ministros, Anexo II

Los terceros usuarios de certificados están obligados a:

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

c) Verificar la validez del certificado.

Obligaciones adicionales

Los terceros usuarios de certificados están obligados también a:

Tomar conocimiento de los términos y condiciones aplicables a los terceros usuarios de los certificados digitales emitidos bajo esta política, publicados en:

- http://www.encodeac.com.ar/firma-digital

2.1.5. - Obligaciones del servicio de repositorio

Son obligaciones del servicio de publicación y repositorio de ENCODE S. A. cumplir con:

Ley Nº 25.506, articulo 21 inc. k)

ENCODE S. A. en su carácter de Certificador Licenciado cumplirá con:

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.

Decreto Nº 2628/02, artículo 34 incisos g), h) y m)

ENCODE S. A. en su carácter de Certificador Licenciado cumplirá con:

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

b) Mantener actualizados los repositorios de certificados revocados por el período establecido por la Autoridad de Aplicación.

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

Obligaciones adicionales

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 Nº 25.506 de Firma Digital, Capítulo IX, existirán dos supuestos de responsabilidad civil

2.2.1. - Responsabilidades del Certificador y el Suscriptor

Existen responsabilidades mutuas entre el certificador licenciado que emite un certificado y el titular de dicho certificado.

Sin perjuicio de las previsiones de la arriba citada ley, y demás legislación vigente, la relación entre ENCODE S. A. y el titular de un certificado se regirá por el acuerdo que se celebre entre ellos, conforme al artículo 37 de la ley 25.506. El modelo de acuerdo está identificado como Acuerdo con Suscriptores y se puede consultar, al igual que otra información disponible, en el sitio web de ENCODE S. A. identificado como:

- http://www.encodeac.com.ar/firma-digital

2.2.2. - Responsabilidades del Certificador ante Terceros usuarios

El Certificador que emita un certificado digital, o lo reconozca en los términos del artículo 16 de la ley 25.506, es responsable de los daños y perjuicios que provoque, por los incumplimientos a las previsiones de la ley, por los errores u omisiones que presenten los certificados digitales que expida, por no revocarlos en legal tiempo y forma cuando así correspondiere y por las consecuencias imputables a la inobservancia de procedimientos de certificación exigibles. Corresponderá al prestador del servicio demostrar que actuó con la debida diligencia.

2.2.3. - Limitaciones de la Responsabilidad

Los Certificadores licenciados no son responsables en los siguientes casos determinados en el artículo 39 de la ley 25.506:

- Por los casos que se excluyan taxativamente en las condiciones de emisión y utilización de sus certificados y que no estén expresamente previstas en la ley;
- Por los daños y perjuicios que resulten del uso no autorizado de un certificado digital, si en las correspondientes condiciones de emisión y utilización de sus certificados constan las restricciones de su utilización;
- Por eventuales inexactitudes en el certificado que resulten de la información facilitada por el titular que, según lo dispuesto en las normas y en los manuales de procedimientos respectivos, deba ser objeto de verificación, siempre que el certificador pueda demostrar que ha tomado todas las medidas razonables.

2.3. - Responsabilidad Financiera

2.3.1. - Responsabilidad financiera del Certificador

ENCODE S. A. será responsable por los daños y perjuicios que provoque, por los incumplimientos a las previsiones de esta Política de Certificación, 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 ENCODE S. A. demostrar que actuó con la debida diligencia.

Las responsabilidades financieras se originan en la ley Nº 25506 y lo establecido por ENCODE S.A. a los efectos de esta Política de Certificación. La parte pertinente de esa norma es transcripta a continuación.

Obligaciones impuestas por la ley Nº 25506, artículo 38

El certificador que emita un certificado digital o lo reconozca en los términos del artículo 16 de la presente ley, es responsable por los daños y perjuicios que provoque, por los incumplimientos a las previsiones de ésta, por los errores u omisiones que presenten los certificados digitales que expida, por no revocarlos, en legal tiempo y forma cuando así correspondiere y por las consecuencias imputables a la inobservancia de procedimientos de certificación exigibles. Corresponderá al prestador del servicio demostrar que actuó con la debida diligencia.

Los certificadores no son responsables en los supuestos del artículo 39 de la ley 25.506.

2.4. - Interpretación y aplicación de las normas

2.4.1. - Legislación aplicable

El bloque normativo aplicable a la presente Política de Certificación está constituido por:

- Ley Nº 25.506 de Firma digital y su Decreto Reglamentario Nº 2628/2002
- Decisión Administrativa Nº 6/2007 de la Jefatura de Gabinete de Ministros y el Decreto Nº 724/06 modificatorio de la reglamentación de la ley Nº 25.506.
- Ley Nº 25326 de Protección de Datos Personales;
- Decreto N° 901/09 que asigna a la Secretaría de Gabinete el carácter de Autoridad de Aplicación del régimen normativo de firma digital.

Supletoriamente se aplicarán el Código Civil y otras normas concordantes dictadas por la autoridad competente.

2.4.2. - Forma de interpretación y aplicación

A los fines de la interpretación y aplicación de la presente Política de Certificación se debe tener en cuenta la normativa que la rige, según el punto anterior.

En caso de reclamos de los usuarios o suscriptores de certificados digitales relacionados con la prestación de servicios de ENCODE S. A., el suscriptor o tercero deberá realizar el correspondiente reclamo en forma fehaciente ante ENCODE y, en caso de haber resultado infructuoso, podrá efectuar una denuncia ante la Autoridad de Aplicación, sin perjuicio de dejar a salvo los derechos de las partes en conflicto de recurrir a la vía judicial cuando así lo creyeren conveniente.

2.4.3. - Procedimientos de resolución de conflictos

En caso de surgir cualquier discrepancia o conflicto interpretativo o de cualquier índole entre las partes, se deberá realizar un reclamo por escrito dirigido a ENCODE S. A., en su condición de Certificador Licenciado.

ENCODE S. A. intentará resolverlos mediante el siguiente procedimiento administrativo a su cargo:

a) Una vez recibida la descripción del conflicto y constatada la divergencia, labrará un acta que deje expresa constancia de los hechos que la motivan y de todos y cada uno de los antecedentes que le sirvan de causa.

b) Dará traslado del acta, mediante notificación fehaciente, a las partes involucradas: Autoridad de Registro delegada (si la hubiera) y/o Suscriptor y/o Tercero usuario. Estas partes dispondrán de un plazo de diez (10) días corridos para ofrecer y producir la prueba que haga a su defensa y aleguen sobre el mérito de la misma.

c) Finalmente, ENCODE S. A. resolverá en un plazo de diez (10) días corridos lo que estime corresponder, conforme a criterios de máxima razonabilidad, equidad y pleno ajuste a la normativa vigente y aplicable en la especie.

Las partes involucradas en el conflicto podrán recurrir ante la Autoridad de Aplicación, previo agotamiento del procedimiento administrativo recién descripto y sin perjuicio de su derecho de acudir directamente a la vía judicial correspondiente.
Los registros electrónicos almacenados bajo condiciones de seguridad razonables y grabados sistemáticamente en un medio permanente e inalterable constituyen plena evidencia del cumplimiento de las obligaciones del certificador y de sus Autoridades de Registros, como así también de las comunicaciones, contratos y pagos hechos entre las partes.

2.5. – Aranceles

Los certificados digitales emitidos bajo la presente política son expedidos a favor de personas físicas y de personas jurídicas a título oneroso, aplicándose aranceles diferenciales asociados conforme a la clase de certificado:

Los aranceles serán publicados en el sitio web ENCODE S. A. al que se accede mediante:

- http://www.encodeac.com.ar/firma-digital/aranceles.html

El solicitante/suscriptor del certificado deberá pagar el arancel de su certificado. Con el comprobante para el pago emitido a ese efecto, podrá abonar en la Autoridad de Registro Central o en los medios de pago que se indican en la siguiente dirección

- http://www.encodeac.com.ar/firma-digital/medio de pago.html

2.6. - Publicación y Repositorios de Certificados y Listas de Certificados Revocados (CRLs)

2.6.1. - Publicación de información del certificador

La publicación de información del Certificador licenciado ENCODE S. A se realiza en sus servidores, y se puede encontrar en el sitio web identificado como:

- http://www.encodeac.com.ar/firma-digital

Se mantiene el repositorio en línea accesible durante las 24hs, los 7 días de la semana, donde se publican las versiones vigentes de los siguientes documentos:

a) Política de Certificación de ENCODE S.A. para personas físicas y jurídicas. En caso de existir, se publicarán las versiones anteriores.

b) Manual de Procedimientos de Certificación en su parte pública. En caso de existir, se publicarán las versiones anteriores.

c) Acuerdo con Suscriptores

d) Política de Privacidad

e) Términos y condiciones con Terceros Usuarios

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

g) Certificado de la "Autoridad Certificante ENCODESIN"

h) Lista de Certificados Revocados (CRL) de la "Autoridad Certificante ENCODESIN".

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

No se publicará la Lista de Certificados Emitidos.

J. G. M. PROY.

2119

2.6.2. - Frecuencia de publicación

Cuando se produzca una actualización de los documentos relacionados con el marco legal u operativo del Certificador, la nueva versión de los documentos mencionados en el punto 2.6.1.- Publicación de Información del Certificador, se publicará dentro de las veinticuatro (24) horas contadas a partir de su aprobación por la Autoridad de Aplicación.

Salvo comunicación en contrario, los certificados ya emitidos continuarán rigiéndose por los documentos vigentes al tiempo de su emisión. Si el cambio resultare de naturaleza tal que torne inviable la continuidad del uso de esos certificados, ENCODE S. A. lo comunicará a todos sus suscriptores quienes tendrán la opción de aceptar el reemplazo de su certificado por el tiempo remanente de su vigencia, sin pago de un nuevo arancel, o pedir la revocación de su certificado.

Además, toda vez que se produzca una revocación, la Autoridad Certificante ENCODESIN emitirá 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

ENCODE S.A. garantiza el acceso permanente, irrestricto y gratuito a la información publicada en su repositorio. No se establecen restricciones al acceso a los sitios de publicación de documentación citada en el punto 2.6.1.

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 ENCODE S. A.

2.7. – Auditorías

EL Ente Licenciante de la Infraestructura de Firma Digital de la República Argentina realiza auditorías ordinarias al Certificador, a la "Autoridad Certificante ENCODESIN" y a sus Autoridades de Registro, a fin de verificar el cumplimiento de los requisitos de licenciamiento.

Esas auditorías tienen por objeto verificar el cumplimiento de los requisitos exigidos para obtener y mantener la condición de Certificador licenciado y la aplicación de las políticas y procedimientos aprobados por el Ente Licenciante para la presente Política de Certificación.

Los temas principales a evaluar en dichas auditorías son:

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) Guía de instalación y funcionamiento de las Autoridades de Registro.

Por su parte, ENCODE S.A. realizará auditorías periódicas a las Autoridades de Registro habilitadas, para verificar el cumplimiento de los requisitos de su habilitación, siendo los temas principales a evaluar:

a) Lo establecido en el documento "Guía de instalación y funcionamiento de las Autoridades de Registro".

b) Las políticas y procedimientos aprobados por el Ente Licenciante para la presente Política de Certificación.

En caso de producirse observaciones en las auditorías realizadas, luego de haber sido debidamente notificadas a ENCODE S.A., ésta tomará 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 Ente Licenciante, es publicada en los sitios mencionados en el apartado "2.6.1. - Publicación de información del certificador".

Así mismo ENCODE SA realizará auditorías periódicas sobre los procesos de la propia AC para verificar el permanente cumplimiento de los requisitos de su habilitación

2.8. - Confidencialidad

Todos los datos correspondientes a las personas físicas y jurídicas a las cuales alcance esta Política de Certificación están sujetos a las estipulaciones de la Ley Nº 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 por juez competente o bien como parte de un proceso judicial o administrativo. La exigencia se extenderá también a toda otra información referida a los

suscriptores de certificados a la que tenga acceso el Certificador o la Autoridad de Registro 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, excepto los datos que figuran en el certificado.-
- Cualquier información almacenada en servidores o bases de datos destinadas a firma digital.
- 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 ENCODE S.A.

La presente lista es de carácter ilustrativo, resultando confidencial toda información del proceso de firma digital que expresamente no señale lo contrario. La regla general es que toda información que no sea considerada como pública revestirá el carácter de confidencial.

Durante el ciclo de vida del certificado, tanto ENCODE S.A. como sus Autoridades de Registro no podrán divulgar los datos de los suscriptores sin su consentimiento. Asimismo, ENCODE S.A. se compromete a hacer público exclusivamente los datos del suscriptor que resulten imprescindibles para el reconocimiento de su firma digital.

Se declaran expresamente como confidenciales:

a) La clave privada de la Autoridad Certificante ENCODESIN. 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 especifica en la presente política.

b) Las claves privadas de los solicitantes y suscriptores. Para garantizar la confidencialidad de las claves de autentificación y firma de los solicitantes o suscriptores, ENCODE S.A. proporcionará los medios para que la generación de dichas claves sólo se realice de modo seguro. Las claves serán generadas por el propio solicitante y almacenadas en un equipo o dispositivo que será preferentemente de tipo criptográfico. A su vez, ni las Autoridades de Registro ni la

Autoridad Certificante ENCODESIN tendrán la posibilidad de generar, almacenar, copiar o conservar información que permita reconstruir o activar las claves privadas de solicitantes y suscriptores.

2.8.2. - Información no confidencial

Se considera información pública y, por lo tanto, no confidencial y accesible por terceros a:

a) Política de Certificación de ENCODE S.A. para personas físicas y jurídicas.

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

c) Acuerdo con Suscriptores.

d) Política de Privacidad.

e) Términos y condiciones con Terceros Usuarios.

f) Certificado de la Autoridad Certificante Raíz de la República Argentina (ACR RA).

g) Certificado de la Autoridad Certificante ENCODESIN

h) Lista de Certificados Revocados (CRL) de la Autoridad Certificante ENCODESIN

i) Información relevante de los informes de la última auditoría realizada.

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 Nº 25.506 no admite la suspensión de certificados.

2.8.4. - Divulgación de información a autoridades judiciales

ENCODE S.A. podrá revelar información confidencial o privada 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

ENCODE S. A. podrá revelar información confidencial si es requerida en el marco de procesos judiciales, administrativos u otros procesos legales, tales como citaciones, interrogatorios, audiencia de posiciones o solicitud de pruebas.

2.8.6. - Divulgación de información por solicitud del suscriptor

Durante el ciclo de vida del certificado el suscriptor en su carácter de titular de datos, previa acreditación de su identidad, tendrá derecho a solicitar y obtener información de sus datos personales incluidos en la base de datos de firma digital del Certificador.

A esos efectos deberá dirigirse en forma fehaciente a la Mesa de Ayuda de ENCODE S. A. donde presentará su solicitud. Dicha petición será resuelta por la Autoridad de Registro Central dentro de los diez (10) días de haber sido recibida. Una vez substanciada la petición será notificada por la Mesa de ayuda al interesado a los fines que pueda ejercer los derechos que le correspondan. En caso que hubiere vencido el plazo sin que el interesado hubiere recibido una respuesta a su petición, podrá iniciar la acción de habeas data, conforme lo indica el artículo 14 de la Ley Nº 25.326 de Protección de los Datos Personales.

Se deja constancia que el Certificador cumple con su obligación de informar a los suscriptores, en su calidad de titulares de datos que, les asiste el derecho a acceder o rectificar sus datos de carácter personal, conforme al artículo citado en el párrafo anterior y al artículo 7 de la Disposición DNPDP Nº 07/08, siempre que el suscriptor aporte la documentación necesaria para validar dicha petición.

2.8.7. - Otras circunstancias de divulgación de información

ENCODE S.A. no divulgará información confidencial a terceros bajo ninguna otra circunstancia que las previstas en los apartados anteriores, excepto en los casos y con el alcance previsto en el artículo 11 de la Ley Nº 25.326 de Protección de los Datos Personales - "Cesión de Datos" -.

2.9. - Derechos de Propiedad Intelectual

ENCODE S. A. 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 ENCODESIN, así como la documentación y contenidos del sitio web de la Autoridad Certificante ENCODESINque se encuentra en:

- http://www.encodeac.com.ar/firma-digital

Asimismo, es titular del derecho de propiedad intelectual de las aplicaciones informáticas propias, excepto los sistemas operativos de soporte informáticos no desarrollados por Encode que cuentan con sus respectivas licencias de uso.

Encode SA es única y exclusiva propietaria de la presente política de certificación, y sus documentos relacionados reservándose todos los derechos de autor establecidos en la legislación vigente de derechos de propiedad intelectual.

3. – IDENTIFICACION Y AUTENTICACION

3.1. - Registro inicial

La Decisión Administrativa Nº 6/2007 de la Jefatura de Gabinete de Ministros establece el "marco normativo de firma digital aplicable al otorgamiento y revocación de las licencias a los certificadores que así lo soliciten". ENCODE S.A. como Certificador Licenciado, se compromete a cumplir con todo lo allí indicado y particularmente con lo establecido en:

a) El artículo 21 inc. a) de la Ley Nº 25.506 y el artículo 34 inc. e) del Decreto Nº 2628/02 relativos a la información a brindar a los solicitantes.

b) El artículo 14 inc. b) de la Ley Nº 25.506 relativo a los contenidos mínimos de los certificados.

ENCODE S.A. en su sitio web

- http://www.encodeac.com.ar/firma-digital

Pone a disposición del Solicitante de un certificado digital, la siguiente información:

c) Las condiciones de utilización del certificado digital;

d) Las características del certificado digital solicitado, entre las cuales se incluirán:

- Identificación del suscriptor
- Vigencia del certificado
- Identificación de la Política de Certificación bajo la cual se emite
- Tipo y Clase de certificado.

e) Las limitaciones a la responsabilidad;

f) Los procedimientos relacionados a las operaciones vinculadas;

g) Los efectos de la revocación de su propio certificado digital y de la licencia que le otorga la Autoridad de Aplicación;

h) Las obligaciones que el suscriptor asume como usuario del servicio de certificación;

i) Los medios a los que el suscriptor puede acudir para solicitar aclaraciones, dar cuenta de mal funcionamiento del sistema, o bien presentar reclamos;

j) De Las Organizaciones con las cuales ENCODE S.A. ha convenido que adopten la utilización de certificados digitales emitidos por la AC Encode SA para sus sistemas de información lo siguiente:

- Identificación de la Organización;
- Características del convenio suscripto con dicha Organización
- Indicación si la Organización actúa como Autoridad de Registro Delegada.

El proceso de solicitud podrá ser iniciado solamente por el Solicitante registrado en la Organización con la que se encuentre relacionado, o desde el portal de suscriptores de ENCODE S.A.

J. G. M. FOLIO 2119

. El tipo de certificado digital que requiere cada Solicitante puede ser de "Persona Física" o de "Persona Jurídica". La generación del par de clave correspondiente al certificado será implementada por software o en un dispositivo criptográfico provisto por el Solicitante, conforme con la lista de dispositivos criptográficos homologados por ENCODE S.A. publicada en

- http://www.encodeac.com.ar/dispositivos-homologados.html

El Solicitante no registrado, deberá registrase en el portal de la Organización con la que se encuentre vinculado y desde allí será direccionado, seleccionando la opción "Solicitud de Certificado" al portal de suscriptor de ENCODE S.A . El Solicitante deberá ingresar la clave y la contraseña que posee en la Organización con la que está vinculado, para ingresar a la aplicación del Certificador.

En caso de contar el solicitante con un dispositivo criptográfico propio deberá colocarlo al inicio de la sesión.

La aplicación le mostrará un formulario de Solicitud de certificado con los datos que ya están registrados en la Organización vinculada y los datos faltantes que él debe completar, en caso de que alguno de los datos registrados en la organización estuviera desactualizado, hubiera cambiado o fuera incorrecto, deberá ser modificado por el solicitante en este mismo formulario. Finalizado el ingreso, el Solicitante confirmará todos los datos proporcionados. Luego, de la lista de lugares para realizar la identificación que le presenta la aplicación, seleccionará la Autoridad de Registro o Autoridad de Registro Delegada más cercana a su domicilio.

Habiendo confirmado los datos de la solicitud y elegido donde realizar la identificación, como medida de seguridad, se envía la solicitud al correo electrónico del titular declarado en la misma, solicitando la confirmación. Únicamente al ser confirmada la recepción del correo electrónico la aplicación procederá a solicitar la elección del proveedor criptográfico con el que se generara el par de claves criptográficas asimétricas. Se realiza la generación del par de claves criptográficas asimétricas y el requerimiento de certificado digital en formato PKCS#10. Si el Solicitante posee un dispositivo criptográfico podrá realizar la generación en el mismo. En caso contrario la generación se hará por software. Generadas las claves, la aplicación del Certificador valida el requerimiento PKCS#10 y genera el PIN de revocación del certificado y envía un nuevo correo electrónico al Solicitante, en la dirección por él informada en su Solicitud. El correo incluye: el resumen criptográfico (huella MD5), los datos de la Autoridad de Registro elegida, con los documentos a presentar ante la misma y su PIN de revocación. Asimismo, se le informará importe y formas de pago disponibles.

Cuando el Solicitante se presenta para su identificación ante el oficial de registro con toda la documentación exigida, procede a firmar el Acuerdo con Suscriptores.

La aprobación de la solicitud de certificado digital estará sujeta al cumplimiento de la verificación de la identidad del Solicitante y al cumplimiento de los requisitos específicos en relación a las características de la clase y tipo de certificado digital solicitado.

El Oficial de Registro, podrá denegar o condicionar la aprobación de la solicitud del interesado hasta el efectivo cumplimiento de los requisitos y condiciones establecidos.

2119

La solicitud para la que no se haya completado el proceso de identificación, caducará a los treinta (30) días de generada.

Una vez identificado el Solicitante y aprobada la solicitud por el Oficial de Registro, la aplicación de la AC ENCODESIN emitirá el certificado y le enviará al Solicitante, por correo electrónico, el aviso correspondiente. El Solicitante descargará e instalará el certificado solicitado.

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

3.1.2.1. - Nombre distintivo para personas físicas

El Nombre Distintivo para los certificados emitidos por ENCODE S. A. para personas físicas está compuesto por los siguientes campos:

a) "Organization Name" (Nombre de la Organización): El nombre y apellido del titular o de la explotación unipersonal con la que se encuentra relacionado el suscriptor, en el caso del titular de un certificado de clase A. El nombre y apellido de la persona física o del titular de la explotación unipersonal que lo autoriza en el caso de certificado de clase B ó C

b) "Common Name" (Nombre): contiene el nombre y apellido que figura en el documento de identidad del suscriptor y coincide con el nombre y apellido registrado para su CUIT o CUIL.

c) "Serial Number" (Nro. de serie): contiene el tipo y número de CUIT o CUIL, expresado como texto y respetando el siguiente formato y codificación: "[tipo]" "[nro]". Si es clase A tendrá CUIT o CUIL. Si es Clase B o C tendrá CUIT o CUIL. Los valores posibles para el campo "tipo" son:

- "CUIT": Clave Única de Identificación Tributaria.
- "CUIL": Clave Única de Identificación Laboral.

d) "Country Name" (Código de país): será el código de país que represente la nacionalidad del Certificador."AR"

e) "Organization Unit": Contiene el tipo y la clase de certificado, por ejemplo "Certificado Persona Física de clase A, B ó C". El tipo igual a persona física y clase es A, B, o C, .-

J. C. M. PROT. 2119

3.1.2.2. - Nombre distintivo para personas jurídicas públicas o privadas

El Nombre Distintivo para los certificados emitidos por ENCODE S.A. para personas jurídicas públicas o privadas está compuesto por los siguientes campos:

a) "Organization Name" (Nombre de la Organización): Nombre de la persona jurídica pública o privada" que figura en el acta de la Inspección de Justicia y en el Registro Público de Comercio, o en la

Autoridad de aplicación correspondiente nacional, o Autoridad de aplicación de Orden Provincial y que coincida con el nombre registrado en su CUIT, a cuyo favor se emitirá el certificado.

b) "Serial Number" (Nro. de serie): contiene la sigla "CUIT", seguida del número que le pertenece a la persona jurídica pública o privada.

c) "Country Name" (Código de país): será el código de país donde está constituida la persona jurídica Certificador. "AR".

d) "Organization Unit": Contiene el tipo y la clase de certificado, Por ejemplo "Certificado Persona Jurídica pública o privada de clase A" . El tipo igual a persona jurídica y clase igual a A.-

e) "CommonName"
Unidad operativa, área o departamento a la que pertenece el suscriptor y razón social de la empresa. Por Ej. "Gerencia – Empresa XX S.A."

f) SubjectAlternativeName : Contendrá los siguiente campos
CommonName: Apellido y Nombre, serialNumber: Tipo de documento y nº de documento, Title: cargo en la Institución.

3.1.3. - Reglas para la interpretación de nombres

Para el caso de las personas físicas, como "Nombre Común" se tomará el nombre y apellido que figure en la documentación de identificación de la persona.

Para el caso de personas jurídicas, como "Organization Name" se tomará la razón social que figura en el acta de la Inspección de Justicia o en el Registro Público de Comercio o en la Autoridad de aplicación correspondiente nacional o en la Autoridad de Aplicación de Orden Provincial y que coincida con el nombre registrado en su CUIT.

En ambos casos, si se presentaran casos de coincidencia de nombres, el método de resolución será la combinación del "Nombre común" con el atributo "Número de serie", formado por la sigla "CUIT" o "CUIL" y el número respectivo para persona física y la combinación de "Organization Name" con el atributo "Número de serie", formado por la sigla "CUIT" y el número respectivo para persona jurídica.-

3.1.4. - Unicidad de nombres

De acuerdo con la Decisión Administrativa Nº 6/2007 de la Jefatura de Gabinete de Ministros y, particularmente, con su Anexo II, "Debe especificarse que el nombre distintivo debe ser único para cada suscriptor, pudiendo existir más de un certificado con igual nombre distintivo si corresponde al mismo suscriptor. El procedimiento de resolución de homonimias deberá estar basado en la utilización del número de documento de identidad

en el caso de personas físicas o el número de identificación tributaria en el caso de personas jurídicas".

La presente Política de Certificación cumple con esta indicación. Si dos o más suscriptores tuvieran el mismo nombre y apellido, o el mismo nombre de persona jurídica, la unicidad queda resuelta por medio de los atributos citados en el punto "3.1.3 Reglas para la interpretación de nombres".

3.1.5. - Procedimiento de resolución de disputas sobre nombres

De acuerdo con la Decisión Administrativa Nº 6/2007 de la Jefatura de Gabinete de Ministros y, particularmente, con su Anexo II, "El certificador podrá reservarse el derecho de tomar todas las decisiones referidas a posibles conflictos sobre la utilización y titularidad de cualquier nombre entre sus suscriptores conforme su normativa al respecto. En caso de conflicto, la parte que solicite el certificado debe demostrar su interés legítimo y su derecho a la utilización de un nombre en particular."

Al respecto, ENCODE S.A. 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

De acuerdo con la Decisión Administrativa Nº 6/2007 de la Jefatura de Gabinete de Ministros y, particularmente, con su Anexo II, "Se indicará que no se podrán incluir marcas comerciales, marcas de servicios o nombres de fantasía como nombres distintivos en los certificados de persona jurídica."

Al respecto, ENCODE S.A. establece que en los certificados para personas jurídicas se incluirá el nombre que figure en el acta emitida por la Inspección General de Justicia, Registro Público de Comercio, Autoridad de Aplicación de Orden Provincial o bien en la Autoridad de Aplicación correspondiente.

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:

- El Solicitante es partícipe directo y necesario en la generación de su par de claves criptográficas asimétricas, utilizando su equipamiento. Las claves criptográficas no quedan almacenadas en los sistemas informáticos de la AC de Encode S.A.

- Durante el proceso de solicitud, se requiere que el Solicitante realice la generación de un par de claves criptográficas asimétricas, dicha operación será realizada desde el equipo del solicitante y en ningún momento de la generación los sistemas informáticos de Encode tienen contacto con la clave privada del solicitante.
- En los casos en los cuales el Solicitante utilice una implementación por software para la generación del par de claves criptográficas asimétricas, usando su perfil en una computadora con la cual también genera la Solicitud, la clave privada podrá quedar almacenada en el disco de esa computadora.
- En los casos en que el Solicitante utilizara un dispositivo criptográfico de su propiedad, las claves son generadas y almacenadas en él.
- Los datos de la Solicitud y el requerimiento con la clave pública del Solicitante, en formato PKCS#10, son enviados a la aplicación del Certificador.
- La aplicación del Certificador valida el requerimiento PKCS#10.
- En caso de ser correcto el formato, la aplicación del Certificador entrega al Solicitante una Solicitud completa incluyendo el resumen criptográfico (huella MD5).
- El Solicitante debe imprimir la Solicitud, para entregar en la Autoridad de Registro, cuando se presenta en el proceso de identificación, demostrando así la posesión de la clave privada.

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

En un todo de acuerdo a lo establecido en el artículo 21 de la ley 25506, artículo 34 inciso a) y sub siguientes del decreto 2628/2 y DA 6/2007 Anexo II 3.1.8 se procederá a identificar a las personas jurídicas públicas o privadas de la forma que se indica.-

El Solicitante del certificado para persona jurídica debe haber completado el requerimiento de solicitud de certificado y creado el par de claves criptográficas, conforme "4.1.2.- Solicitud de certificado para persona jurídica" y, previo pago del arancel correspondiente, se presentará en la AR seleccionada, con la documentación detallada en la guía del solicitante; a modo ilustrativo se mencionan algunos de los comprobantes a presentar:

a) El representante legal, apoderado o administrador de la persona jurídica Solicitante del certificado se presenta ante el Oficial de

Registro con los documentos que se detallan más abajo con copias certificadas por Escribano Público los que correspondieren, tal cual se indica en la Guía del Solicitante :

b) Estatuto o Contrato Social correspondiente a la Persona Jurídica ;

c) Acta de directorio o documento que acredite la representación invocada y su documento de identidad,

d) Constancia de inscripción en el Registro Público de Comercio,

e) Constancia de inscripción en AFIP;

f) DNI de todos los socios, en caso de sociedades irregulares,

g) Acta de distribución de cargos,

h) Poder General Amplio o Poder especial que autoriza la solicitud de certificado de firma digital. Se hace saber al Solicitante que se encuentra en la "Guía del Solicitante" el modelo de poder especial requerido a los fines de solicitar un certificado de firma digital.

i) Solicitud de certificado impresa,

j) Recibo que acredita el pago del certificado correspondiente.

k) A los fines de que el Solicitante tome conocimiento de la documentación que requiere ser acompañada para su identificación y la identificación de la persona jurídica que representa, se sugiere consultar la "Guía del Solicitante" que se encuentra publicada en el sitio web

http://www.encodeac.com.ar/firma-digital/guia del solicitante.html

El Solicitante será atendido por un Oficial de Registro, quien verificará su identidad, la documentación que presenta y el resumen criptográfico (huella MD5) vinculado con la Solicitud, así como toda otra información contenida en la Solicitud.

J. G. M. PROY.

Si la identificación ha sido satisfactoria, el Solicitante firma dos ejemplares impresos del "Acuerdo con Suscriptores", quedando uno en poder del Solicitante y el otro en poder de la Autoridad de Registro correspondiente.

2119

El Oficial conserva para el armado de la carpeta del suscriptor la documentación presentada como respaldo del proceso de identificación.

Recibida la documentación en la AR, el Oficial de Registro procederá a efectuar el control de la documentación. Luego cargará en la aplicación de la Autoridad de Registro la confirmación de los documentos recibidos y determinará la aceptación o rechazo de la Solicitud.

En caso de aprobar la Solicitud, el Oficial de Registro, firmará la misma con su certificado habilitado en la aplicación de la AR.

Finalmente, en caso de aprobación, la aplicación enviará un mail al Solicitante a los fines de hacerle saber que el certificado está listo para su descarga e instalación.

El Oficial de Registro arma la carpeta de respaldo de la identificación de la persona jurídica Solicitante. Esta contiene la Solicitud de Certificado, y todos los documentos presentados de acuerdo a lo exigido en la "Guía del Solicitante" y el Acuerdo con Suscriptores firmado.

Si la Solicitud es rechazada o dada de baja por falta de identificación, la aplicación le informará la condición al Solicitante por medio de un correo electrónico.

Para los casos de renovación, la Autoridad de Registro podrá requerir, ante dudas, respecto de la verificación realizada con anterioridad, que el Solicitante/Suscriptor se presente nuevamente para acreditar identidad.

3.1.9. - Autenticación de la identidad de personas físicas

Es requisito previo proceder a completar los datos de la Solicitud del certificado digital y a la creación del par de claves criptográficas, conforme surge del punto "4.1.1.- Solicitud de certificado para persona física". La exhibición del pago del arancel del certificado deberá realizarse, en forma previa a su emisión.

El Solicitante deberá presentarse personalmente frente a la Autoridad de Registro correspondiente, donde acreditará fehacientemente su identidad, acompañando la siguiente documentación:

a) Documento de Identidad original y fotocopia (DNI, LE, LC, Pasaporte o Documento Extranjero (si correspondiera).

b) Comprobante de CUIT/CUIL expedido a su nombre y vigente.

c) Solicitud completa, impresa.

d) Recibo de pago de arancel del certificado solicitado correspondiente.

e) En caso de Apoderado, presentará Poder General amplio o especial para solicitar firma digital, debiendo éste exhibir su documento de identidad.

f) Constancia de inscripción en AFIP para verificar la condición de empleador del titular del certificado.

El Solicitante será atendido por un Oficial de Registro quien verificará su identidad, la documentación que presenta y el resumen criptográfico (huella MD5) vinculado con la Solicitud, así como toda otra información contenida en la Solicitud.

Si la identificación ha sido satisfactoria, el Solicitante firma dos ejemplares impresos del "Acuerdo con Suscriptores", quedando uno en poder del Solicitante y otro en la Autoridad de Registro.

Devuelve los originales de todos los documentos y conserva los duplicados.

Luego cargará en la aplicación de la Autoridad de Registro la confirmación de los documentos recibidos y determinará la aceptación o rechazo de la Solicitud.

En caso de aprobar la solicitud, el Oficial de Registro, firmará la misma con su certificado habilitado en la aplicación de la AR.-

Finalmente, en caso de aprobación de la Solicitud, la aplicación enviará un mail al Solicitante a los fines de hacerle saber que el certificado está listo para su descarga e instalación.

El Oficial de Registro arma la carpeta de respaldo de la identificación de la persona física Solicitante. Esta contiene la Solicitud de Certificado, los duplicados de todos los documentos presentados y el Acuerdo con Suscriptores firmado.

Si la Solicitud es rechazada o dada de baja por falta de identificación, la aplicación le informará esta condición al Solicitante por medio de un correo electrónico.

Para los casos de renovación, la Autoridad de Registro podrá requerir, ante dudas, respecto de la verificación realizada con anterioridad, que el Solicitante/Suscriptor se presente nuevamente para acreditar identidad.

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

No está previsto el cambio de claves de un certificado. En caso de que el Suscriptor requiera generar un nuevo par de claves se deberá revocar el certificado y emitir uno nuevo en su reemplazo. Para ello deberá realizar el proceso de Solicitud completo y la presentación ante el Oficial de Registro para validar su identidad.

J. G. M. PROY.
2119

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 después de una revocación, deberá realizar el proceso de Solicitud completo y la presentación frente al Oficial de Registro para validar su identidad.

3.4. - Requerimiento de revocación

La revocación podrá ser iniciada por el Suscriptor, por la Autoridad de Registro o por la AC.

Los suscriptores podrán solicitar la revocación de su certificado ingresando a la aplicación del Certificador desde:

- http://www.encodeac.com.ar/firma-digital/revocacion.html

Este sitio se encuentra disponible las 24 horas los 7 días de la semana, durante todo el año, lo que permite servicios de revocación en horarios no habituales de jornada laboral, como así también fines de semana y feriados. La solicitud de revocación se procesa automáticamente de acuerdo a lo establecido en el punto 4.4.4. - Plazo para la Solicitud de revocación.
El Suscriptor que inicia la revocación se debe identificar en el portal con su clave de organización y luego con su Pin de revocación, obtenido durante el proceso de Solicitud, inicia el proceso de revocación de certificado.
En el caso de pérdida del PIN de revocación se deberá solicitar en el portal del Suscriptor el reenvío del mismo. Éste se enviará a la dirección informada por el Suscriptor, en forma automática.

La Autoridad de Registro o la AC de ENCODE S.A., podrán iniciar de oficio o por decisión del Responsable de ENCODE S.A., la revocación de certificados, según lo indicado en el "4.4.1. - Causas de revocación".

La Autoridad de Registro o la AC de ENCODE S.A., con la documentación relacionada con la revocación, procede a ingresar a la aplicación del Certificador con su clave, selecciona el certificado a revocar que le pertenece al suscriptor e inicia, con su solicitud, el proceso automático de revocación. Deja asentado en los registros informáticos de la AR la revocación efectuada.

Para aquellos suscriptores relacionados con una Organización, ésta se obliga a: 1) notificar a la Autoridad de Registro de toda modificación de la situación del suscriptor que llevaría a inhabilitarlo como suscriptor de un certificado conforme a la presente Política de Certificación, o bien la modificación de los datos del suscriptor que llevarían a modificar la información contenida en el certificado expedido a favor de dicho suscriptor y 2) solicitar el requerimiento de revocación inmediata del certificado. También se revocarán los certificados de estos suscriptores en el caso de finalización de la relación entre la Organización y ENCODE S.A.

J. C. M. PROT. 2119

Encode SA informará a los suscriptores en caso del término de la relación entre la organización a la que se encuentra vinculadas los mismos y Encode SA, mediante la publicación en el portal de suscriptores de la organización y con una notificación a la casilla de correo electrónica que informó oportunamente.-

4. - CICLO DEL CERTIFICADO: REQUERIMIENTOS OPERATIVOS

4.1. - Solicitud de certificado

4.1.1. - Solicitud de certificado de persona física

El proceso de solicitud de emisión de certificado debe ser iniciado exclusivamente por el Solicitante, quien luego, debe acreditar fehacientemente su identidad según se indica en "3.1.9. - Autenticación de la identidad de personas físicas".

Para poder efectuar la Solicitud de un certificado, el Solicitante debe:

- Contar con la clave de su Organización para acceder a la aplicación del Certificador. El Solicitante deberá darse de alta en el sistema de su Organización procediendo a su registración. Si ya se encontrase registrado deberá ingresar su clave y su contraseña en el sitio de su Organización y seleccionar la pestaña "Solicitud de certificado" para ingresar al portal del Suscriptor.
- Contar con su dirección de correo electrónico e informarla a los fines de ser notificado en el proceso de solicitud y emisión de su certificado.
- Cumplir con los requisitos mínimos de configuración de hardware y software detallados en la "Guía del Solicitante" que se encuentra en:

  http://www.encodeac.com.ar/firma-digital/guia_del_solicitante.html

- En caso de contar el Solicitante con un dispositivo criptográfico propio, de los modelos homologados por el Certificador, deberá colocarlo al inicio de la sesión.
- El sistema seleccionara automáticamente el tipo de certificado digital que requiere cada Solicitante de "Persona Física" y la clase del mismo, las cuales podrán ser A, B ó, C.
- La aplicación, mostrara el formulario de Solicitud de persona física con los datos que tuviere almacenados respecto a la Organización vinculada con dicha solicitud, en relación a la organización del Solicitante, en caso de que alguno de los datos registrados en la organización estuviera desactualizado, hubiera cambiado o fuera incorrecto, deberá ser modificado por el solicitante en este mismo formulario y confirmará los mismos. Luego le presentara el panel para ingresar los datos de la persona física.

- Si el Certificado solicitado fuese de tipo B ó C se le pedirá indicar la relación con el titular del certificado clase A que lo autoriza.
- Completados los datos de la Solicitud, el Solicitante deberá confirmarlos.
- El sistema a continuación desplegará las Autoridades de Registro Central y Delegadas de ENCODE S.A., debiendo el Solicitante proceder a elegir libremente la más conveniente para realizar su identificación.
- Habiendo confirmado los datos de la solicitud y elegido donde realizar la identificación, como medida de seguridad, se envía la solicitud al correo electrónico del titular declarado en la misma, solicitando la confirmación.
- Únicamente al ser confirmada la recepción del correo electrónico la aplicación procederá a solicitar la elección del proveedor criptográfico con el que se generara el par de claves criptográficas asimétricas.
- Se realiza la generación del par de claves criptográficas asimétricas y el requerimiento de certificado digital en formato PKCS#10. Si el Solicitante posee un dispositivo criptográfico podrá realizar la generación en el mismo. En caso contrario la generación se hará por software.
- Generadas las claves, la aplicación del Certificador valida el requerimiento PKCS#10 y genera el PIN de revocación del certificado y envía un nuevo correo electrónico al Solicitante, en la dirección por él informada en su Solicitud.
- El correo incluye: la Solicitud con el resumen criptográfico (huella MD5), los datos de la Autoridad de Registro con los documentos a presentar ante la misma y su PIN de revocación. Asimismo, en los casos que corresponda se le informará importe y formas de pago disponibles.
- En el caso de solicitarse un certificado de clase B ó C, dicha Solicitud de Certificado generada, es colocada en la bandeja de documentos del titular de certificado clase A relacionado, para que sea firmada por éste con su correspondiente certificado, autorizando a la solicitud del certificado de clase B ó C. El titular del certificado clase A, recibirá un correo electrónico con la notificación de que existe una solicitud de certificado clase B ó C pendiente de firma en su bandeja de documentos la cual podrá ser accedida desde este correo electrónico o desde el portal del suscriptor en la opción "Bandeja Documentos"
- Si la Solicitud es rechazada se le informa al Solicitante en su dirección de correo electrónico.
- Cumpliendo el Solicitante con presentarse en la AR elegida, la aprobación de la Solicitud de certificado digital estará sujeta a cubrir los

requerimientos para la verificación de la identidad del Solicitante y los requisitos específicos en relación con las características del certificado digital solicitado.

- En caso de aprobar la solicitud, el Oficial de Registro, firmará la misma con su certificado habilitado en la aplicación de la AR.
- Finalmente, en caso de aprobación de la Solicitud, la aplicación enviará un mail al Solicitante a los fines de hacerle saber que el certificado está listo para su descarga e instalación.
- El Oficial de Registro arma la carpeta de respaldo de la identificación de la persona física Solicitante. Esta contiene la Solicitud de Certificado, los duplicados de todos los documentos presentados en un todo de acuerdo con lo especificado en la "Guía del Solicitante" y el Acuerdo con Suscriptores firmado.

4.1.2. - Solicitud de certificado de persona jurídica

El proceso de solicitud de emisión de certificado debe ser iniciado exclusivamente por el representante legal, administrador o apoderado de la persona jurídica Solicitante, quien luego deberá acreditar fehacientemente su identidad según se indica en "3.1.8. - Autenticación de la identidad de personas jurídicas públicas o privadas".

Para poder efectuar la solicitud de un certificado, el Solicitante debe:

- Contar con la Clave dada por la Organización con la que se encuentra vinculado, para acceder a la aplicación del Certificador. El Solicitante deberá darse de alta en el sistema de la Organización procediendo a su registración. Si ya se encontrase registrado deberá ingresar su clave y su contraseña, seleccionar la opción "Solicitud de Certificado" para ingresar a la aplicación del Certificador.
- Contar con su dirección de correo electrónico e informarla a los fines de ser notificado en el proceso de solicitud y emisión de su certificado
- Cumplir con los requisitos mínimos de configuración de hardware y software detallados en la "Guía del Solicitante" que se encuentra en:
  - http://www.encodeac.com.ar/firma-digital/guia del solicitante.html
- El proceso de solicitud podrá ser iniciado solamente por el apoderado, administrador o representante legal de la persona jurídica a favor de la cual se emitirá el certificado, ingresando desde el sitio web de la Organización. La clase de certificado digital que requiere el Solicitante podrá ser A, el tipo es de "Persona Jurídica" y será asignado por la aplicación en función de los datos del Solicitante.

- La aplicación del Certificador verifica que la estación de trabajo del Solicitante cumple con los requerimientos técnicos mínimos. En caso de no cumplimentar los requerimientos técnicos mínimos el sistema le indicará las actualizaciones necesarias para solucionar dichos inconvenientes técnicos y de persistir los mismos deberá dirigirse a la A.R. Central o A.R. delegada donde se le proporcionará un equipo preparado para que pueda realizar desde el mismo la suscripción utilizando un dispositivo criptográfico propio para generación y el almacenamiento de su par de claves, y en ningún caso existirá contacto de la AR o AC con la clave privada del solicitante.
- En caso de contar el Solicitante con un dispositivo criptográfico propio, deberá colocarlo al inicio de la sesión.
- La aplicación le presenta la pantalla con el formulario de Solicitud de Certificado de Persona Jurídica. La aplicación le traerá los datos que tuviere almacenados la Organización vinculada, en relación a la persona jurídica a favor de la cual se emitirá el certificado requerido, debiendo el solicitante proceder a su confirmación.En caso de que alguno de los datos registrados en la organización estuviera desactualizado, hubiera cambiado o fuera incorrecto, deberá ser modificado por el solicitante en este mismo formulario luego de lo cual confirmará los mismos.
- A continuación le solicita todos los datos del Solicitante en su calidad de representante legal, administrador o apoderado de la persona jurídica.
- Completada la Solicitud, el Solicitante deberá confirmar todos los datos presentes en la misma.
- El sistema a continuación desplegará la Autoridad de Registro Central y la Autoridad de Registro Delegada, si correspondiere, debiendo el Solicitante proceder a elegir libremente la opción más conveniente a los efectos de completar su identificación.
- Habiendo confirmado los datos de la Solicitud y elegido el lugar para la identificación, como medida de seguridad, se la envía al correo electrónico declarado en la solicitud, solicitando la confirmación.
- Únicamente al ser confirmada la recepción del correo electrónico la aplicación procederá a solicitar la elección del proveedor criptográfico con el que se generara el par de claves criptográficas asimétricas.
- Se realiza la generación del par de claves criptográficas asimétricas y el requerimiento de certificado digital en formato PKCS#10. Si el Solicitante posee un dispositivo criptográfico podrá realizar la generación en el mismo. En caso contrario la generación se hará por software

- Generadas las claves, la aplicación del Certificador valida el requerimiento PKCS#10 y genera el PIN de revocación del certificado y envía un nuevo correo electrónico al Solicitante, en la dirección por él informada en su Solicitud.
- El correo incluye: la Solicitud con el resumen criptográfico (huella MD5), los datos de la ubicación de la identificación con los documentos a presentar ante la misma y su PIN de revocación. Asimismo, se le informará importe y formas de pago disponibles.
- La aprobación de la solicitud de certificado digital estará sujeta al cumplimiento de los requerimientos para la verificación de la identidad del Solicitante y al cumplimiento de los requisitos específicos en relación a las características del certificado digital solicitado.
- En caso de aprobar la solicitud, el Oficial de Registro, firmará la misma con su certificado habilitado en la aplicación de la AR.
- Finalmente, en caso de aprobación de la Solicitud, la aplicación enviará un mail al Solicitante a los fines de hacerle saber que el certificado está listo para su descarga e instalación.
- El Oficial de Registro arma la carpeta de respaldo de la identificación de la persona jurídica Solicitante. Esta contiene la Solicitud de Certificado, los duplicados de todos los documentos presentados y el Acuerdo con Suscriptores firmado.

4.1.3. – Solicitud de renovación de certificado de persona física

La aplicación del Certificador brinda un servicio de alerta al suscriptor persona física, respecto a la próxima expiración de su certificado digital, a partir de los treinta días anteriores a la fecha de vencimiento.

El proceso de solicitud de renovación deberá ser iniciado exclusivamente por el suscriptor, antes de vencer el período de validez de su certificado y en posesión de su clave privada.

Los datos del certificado deben ser los mismos. En caso contrario se debe revocar y solicitar un nuevo certificado de acuerdo con el punto 4.1.1 Solicitud de certificado de persona física.

En la renovación del certificado no será necesario realizar nuevamente la identificación en las oficinas del Certificador.

Para realizar la renovación deberá acceder al portal del suscriptor desde la siguiente dirección:

- http://www.encodeac.com.ar/firma-digital/renovacion.html

El período de validez es indicado en 6.3.2 - Periodo de uso de clave pública y privada.

Una vez ingresado al sitio web el sistema le mostrará la lista de certificados vigentes de el solicitante, deberá seleccionar el que se deba renovar, la forma de pago y confirmar la solicitud. Se generará un nuevo requerimiento PKCS#10 reutilizando el par de claves del certificado que se está renovando. Finalmente la aplicación enviará un mail al Solicitante a los fines de hacerle saber que el certificado está listo para su descarga e instalación.

4.1.4. – Solicitud de renovación de certificado de persona jurídica

La aplicación del Certificador brinda un servicio de alerta al suscriptor persona jurídica respecto a la próxima expiración de su certificado digital, a partir de los treinta días anteriores a la fecha de vencimiento.

Los datos del certificado deben ser los mismos. En caso contrario se debe revocar y solicitar un nuevo certificado de acuerdo con el punto 4.1.2 Solicitud de certificado de persona jurídica.

El proceso de solicitud de renovación deberá ser iniciado exclusivamente por el representante legal o apoderado del suscriptor, antes de vencer el período de validez de su certificado y en posesión de su clave privada.

En la renovación del certificado no será necesario realizar nuevamente la identificación en las oficinas del Certificador. Para realizar la renovación deberá acceder al portal del suscriptor desde la siguiente dirección:

- http://www.encodeac.com.ar/portal-suscriptor/renovacion.html

El período de validez es indicado en 6.3.2 - Periodo de uso de clave pública y privada.

Una vez ingresado al sitio web el sistema le mostrará la lista de certificados vigentes del solicitante, deberá seleccionar el que se deba renovar, la forma de pago y confirmar la solicitud. Se generará un nuevo requerimiento PKCS#10 reutilizando el par de claves del certificado que se está renovando. Finalmente la aplicación enviará un mail al Solicitante a los fines de hacerle saber que el certificado está listo para su descarga e instalación.

J. G. M. PROT. 2119

4.2. - Emisión del certificado

Cumplidos los recaudos del proceso de identificación y autenticación de acuerdo con esta Política, y una vez aprobada la Solicitud por la Autoridad de Registro, la Autoridad Certificante ENCODESIN emite el correspondiente certificado, firmándolo digitalmente con su clave privada.

El sistema pone el certificado en el Portal del Suscriptor, a disposición de su titular y le comunica esa disponibilidad por correo electrónico. El Portal del Suscriptor se encuentra en:

- http://www.encodeac.com.ar/firma-digital/portal-suscriptor.html

En este sitio web cada Solicitante puede acceder únicamente a su propia información.

4.3. - Aceptación del certificado

Una vez notificado de la emisión de un certificado a su nombre, el Suscriptor o bien su representante legal o apoderado en caso de tratarse de certificados de personas jurídicas, deberá controlar su contenido y descargar el certificado desde el Portal del Suscriptor.

En caso de que existiera algún error u omisión en los datos del suscriptor contenidos en el certificado, deberá revocarlo con su PIN de revocación desde el Portal del Suscriptor, como se indica en 3.4 Requerimiento de revocación.

En caso de formular un reclamo de no aceptación del certificado antes de descargar el mismo deberá realizarlo dentro de las 48 horas de la notificación de ENCODE de la puesta a disposición en el portal del suscriptor del certificado a su nombre

Ante la ausencia de reclamos a la Autoridad de Registro por parte del Suscriptor, en cuanto a los datos del certificado, se acepta la exactitud del contenido del certificado desde el momento de su notificación y el Suscriptor asume la totalidad de las obligaciones y responsabilidades establecidas por esta Política de Certificación.

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 ENCODESIN revocará un certificado por ella emitido, en los casos en que:

a) Lo solicite el titular del certificado por cualquier causa, incluida el haber tomado conocimiento de que su clave privada esté comprometida y haya dejado de ser segura.

b) ENCODE S.A. determine que el certificado fue emitido en base a una información falsa, que en el momento de la emisión hubiera sido objeto de verificación.

c) ENCODE S.A. determine que los procedimientos de emisión y/o verificación han dejado de ser seguros.

d) La Organización que haya adoptado el uso de certificados de firma digital emitidos por la AC de ENCODE S. A. , notifique a la Autoridad de Registro que la información contenida en el certificado ha dejado de ser exacta.

e) Fuere solicitado por resolución judicial o de la Autoridad de Aplicación de la Ley Nº 25.506 debidamente fundada.

f) ENCODE S.A. 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).

g) Por fallecimiento del titular, declaración judicial de ausencia con presunción de fallecimiento o declaración judicial de incapacidad, en el caso de persona física comunicada fehacientemente por sus herederos o autoridad judicial competente a ENCODE SA.

h) Por cese del representante legal y su sustituto, en el caso de personas jurídicas comunicada fehacientemente por el nuevo representante legal, administrador o apoderado de la persona jurídica a ENCODE SA.

i) Por cambio en los atributos de un certificado, aun cuando hubieran sido válidos al tiempo de su emisión.

j) Por cese de la existencia de la Persona Jurídica, comunicada fehacientemente por el representante legal de la misma a ENCODE S.A.

k) Por cese de la Licencia del Certificador.

l) Por haberse resuelto el contrato que ENCODE S.A. hubiera suscripto con la Organización a la cual perteneciese el Suscriptor, o lo convenido entre las partes, en el caso que corresponda.

m) Los certificados clase B por finalización de la relación de dependencia con el titular del certificado A

n) Los certificados clase C por cese del vínculo contractual con el titular del certificado clase A

En caso de revocación de un certificado de persona física o jurídica de clase A por las causales mencionadas, los certificados de persona física clase B ó C relacionados deberán ser revocados si el titular del certificado A lo solicitara expresamente, caso contrario su revocación queda a criterio de ENCODE SA.

4.4.2. - Autorizados a solicitar la revocación

Los siguientes actores podrán solicitar la revocación de un certificado emitido por la Autoridad Certificante ENCODESIN:

a) El Suscriptor del certificado, si se trata de una persona física.

b) El representante legal, administrador o apoderado, si se trata de una persona jurídica.

c) La Autoridad de Registro.

d) La Autoridad de Aplicación.

e) La Autoridad Judicial competente.

f) El Certificador Licenciado.

g) El titular del certificado A para solicitar la revocación de los certificados clase B ó C vinculados.

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"

Los suscriptores podrán solicitar la revocación de su certificado ingresando a la aplicación del Certificador desde:

- http://www.encodeac.com.ar/firma-digital/revocacion.html

Este sitio se encuentra disponible las 24 horas los 7 días de la semana, durante todo el año, lo que permite servicios de revocación en horarios no habituales de jornada laboral, como así también fines de semana y feriados.

Las Autoridades de Registro conservarán como documentación probatoria toda solicitud de revocación y el material probatorio vinculado, el que será archivado en la carpeta de identificación del Solicitante/Suscriptor. Se registraran en los registros informáticos de la AR la revocación.

Los suscriptores o sus representantes serán notificados en sus respectivas direcciones de correo electrónico del cumplimiento del proceso de revocación.

La revocación se reflejará en la próxima Lista de Certificados Revocados, cuando sea generada de acuerdo con lo especificado en el punto "2.6.2. - Frecuencia de publicación".

FOLIO 158

4.4.4. - Plazo para la solicitud de revocación

La recepción de la solicitud de revocación está disponible 7 días de la semana x 24 hs. a través de la aplicación del Certificador desde:

- http://www.encodeac.com.ar/firma-digital/revocacion.html

Esta solicitud será procesada de inmediato, sin intervención de la Autoridad de Registro.

En caso de que el Suscriptor se presente personalmente ante la Autoridad de Registro, la solicitud de revocación será ingresada por el Oficial de Registro y también procesada de inmediato.

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.

4.4.9. - Frecuencia de emisión de listas de certificados revocados

La Autoridad Certificante ENCODESIN genera y publica periódicamente una única lista conteniendo todos los certificados revocados por ella, en forma acumulativa, en formato del CRL X.509 v2, sin superar las veinticuatro (24) horas entre publicaciones.

J. G. M. PROY. 2119

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

Para determinar el estado de validez de un certificado, se debe 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 de CRLs

emitidas previamente son mantenidas en los archivos internos del Certificador. Si no se pudiera obtener una CRL actualizada, quien busca la verificación deberá optar entre rechazar el documento firmado digitalmente, aceptarlo bajo exclusiva responsabilidad de quien consulta o postergar la decisión hasta obtener una CRL actualizada.

Las aplicaciones habilitadas por ENCODE S.A se encuentran publicadas en la url:

http://www.encodeac.com.ar/firma-digital/aplicaciones.pdf

Las mismas verifican en forma automática el estado de validez de los certificados utilizados por los suscriptores.

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

ENCODE S. A. 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.

Todas las aplicaciones propias de ENCODE S.A. donde se utilizan los certificados emitidos por la AC ENCODESIN realizan la consulta sobre la lista de Certificados Revocados, en forma automática.

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

En todas las situaciones que involucren el compromiso de la clave privada del Suscriptor, éste deberá revocar su certificado. Podrá hacerlo por alguna de las vías indicadas en el punto "3.4. – Requerimiento de revocación".

4.5. - Procedimientos de Auditoría de Seguridad

La Autoridad Certificante mantiene registros de auditoría ("logs") de todas las operaciones que realiza, protegiendo su integridad en medios de almacenamiento seguros y conservándolos por 10 años como mínimo.

Los registros de auditoría son analizados por ENCODEMON (servicio que registra en forma automática las alteraciones en el funcionamiento de la instalación)en las tareas de monitoreo habitual del funcionamiento de los sistemas, las aplicaciones y los procesos.

Con el propósito de mantener la seguridad de los sistemas, el responsable de Seguridad Informática realiza evaluaciones periódicas sobre los informes de ENCODEMON Asimismo, atendiendo a lo expresado en el punto 2.7 Auditoría, se mantendrán registros no informatizados de toda aquella información soportada en papel.

4.6. - Archivo de registros de eventos

El Certificador genera, mantiene y conserva registros de eventos sobre cada una de las actividades que comprenden los componentes del proceso de certificación.

La información registrada abarca:

- Fecha y hora del registro
- Número de serie o secuencia del registro
- Tipo de registro
- Fuente del registro
- Identificación de la entidad que efectuó el registro

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

J. G. M. PROY.

2119

	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 nueva o renovación 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) Esta actividad estará bajo la responsabilidad del suscriptor b) El certificador solo registra el uso del dispositivo
Información relacionada con la solicitud de Certificados	a) Tipos de documentos de identificación presentados por el solicitante b) Otra información de identificación c) Ubicación del archivo de las copias de las solicitudes de certificados y de los documentos de identificación d) Identificación de la entidad que recibe y acepta la solicitud e) Método utilizado para validar los documentos de identificación f) Identificación de la Autoridad de Registro
Eventos de seguridad	a) Lecturas y/o escrituras en archivos sensibles de seguridad

J. G. M. PROY.

2119

	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 ENCODE S. A. y una Autoridad de Registro Delegada o personal relacionado con el proceso de certificación h) Accesos a los componentes del sistema de la Autoridad Certificante ENCODESIN i) Eventos o situaciones no previstas

4.7. - Cambio de claves criptográficas

Las claves criptográficas de la Autoridad Certificante ENCODESIN son generadas con motivo del licenciamiento de la presente Política de Certificación y tendrán una duración de 5 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 ENCODESIN, dará origen a la emisión de un nuevo certificado, por parte de la Autoridad Certificante Raíz de la República Argentina operada por la Autoridad de Aplicación.

Un año antes del vencimiento previsto del certificado de la Autoridad Certificante ENCODESIN se solicitará la renovación de la licencia de la Política de Certificación y el certificado correspondiente.

4.8. - Plan de contingencia y recuperación ante desastres

El Plan de Contingencia de ENCODE S. A. como Certificador Licenciado establece los procedimientos y actividades relacionados con la continuidad del servicio de certificación de firma digital y será de aplicación desde el momento de la declaración de la contingencia hasta la restauración de la operatoria normal.

ENCODE S.A. cuenta con un sitio de contingencia propio, con las características necesarias de acuerdo con los estándares de seguridad y las protecciones correspondientes. El acceso

al sitio es las 24 horas, los 365 días del año, lo que le permite asegurar la continuidad de sus servicios.

Están previstos mecanismos de prueba y simulación con frecuencia periódica 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 mantener el entrenamiento del personal y minimizar el tiempo de recuperación de la continuidad del negocio.

4.9. - Plan de Cese de Actividades

El Certificador puede cesar en sus actividades. Este hecho se podrá producir a partir de la manifestación del Directorio de ENCODE S. A., como máxima autoridad de la empresa, sobre su decisión de proceder al cese de actividades, ya sea por razones de índole económica, empresaria o de seguridad. También podrá ser motivado por la cancelación de la licencia, dispuesta por la Autoridad de Aplicación o por disolución de la sociedad.

ENCODE S. A., a fin de contemplar esta situación elaboró el documento "Plan de Cese", con las estrategias y procedimientos a seguir desde la declaración del cese de actividades hasta la inhabilitación lógica y física de la Autoridad Certificante ENCODESIN.

Primeramente el Directorio comunicará la decisión a la Autoridad de Aplicación y determinara los procedimientos de revocación aplicables en estos casos de acuerdo con el artículo 22 de la ley 25506 y según su plan de cese de actividades, excepto que la Autoridad de aplicación indique otro curso de acción.-

Ante la declaración del cese de los servicios de certificación, ENCODE S. A. procederá a la publicación de dicha circunstancia a través del sitio web:

- http://www.encodeac.com.ar/firma-digital

También se publicará en un medio de difusión provincial o nacional y en el Boletín Oficial.

Toda información digital será resguardada por ENCODE S. A. 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 esta sociedad, la custodia de los registros y archivos pasarán a manos de la Sociedad Liquidadora constituida a esos efectos, salvo opinión en contrario de la Autoridad de Aplicación de Firma Digital de la República Argentina.

J. G. M. PROY.

2119

5. - CONTROLES DE SEGURIDAD FÍSICA, FUNCIONALES Y PERSONALES

5.1. - Controles de seguridad física

Los sistemas centrales de la Autoridad Certificante ENCODESIN se encuentran en el Sitio de Máxima Seguridad (SMS) de ENCODE S.A., el cual cuenta con controles de seguridad física que protegen las instalaciones informáticas de la Autoridad Certificante de accesos no autorizados y garantizan la continuidad de sus operaciones.

Algunas de sus características comprenden:

a) Monitoreo ambiental de temperatura y humedad.

b) Prevención contra incendios.

c) Aislamiento a altas temperaturas externas.

d) Estructura sólida de bóveda.

e) Prevención contra explosiones, derrumbes y sismos.

f) Prevención temprana de incendios.

g) Sistemas de refrigeración y control de humedad.

h) Sistemas de suministro de energía ininterrumpido.

i) Sistema de generación de energía alternativo.

j) Sistemas de conectividad redundantes.

k) Control de acceso con tarjetas de aproximación e identificación biométrica.

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

El acceso al SMS está limitado al personal autorizado y estrictamente necesario para el mantenimiento y administración de los sistemas de la AC ENCODESIN de ENCODE S.A.

El almacenamiento de los datos de activación de la clave privada de la Autoridad Certificante ENCODESIN se realiza cumpliendo con los niveles de seguridad de acceso físico establecidos por la normativa vigente.

Los controles de Seguridad Física de las Autoridades de Registro se encuentran contempladas en el documento interno" Guía de instalación y funcionamiento de las Autoridades de Registro".

5.2. - Controles Funcionales

Los controles funcionales son realizados por personal de ENCODE S. A. sobre todos los roles del Certificador, verificando el cumplimiento de las responsabilidades de cada uno de ellos, de acuerdo a lo establecido en la presente política y en los documentos internos:

"Roles y Funciones" y "Guía de instalación y funcionamiento de las Autoridades de Registro".

Los roles son asignados por el Directorio de ENCODE S. A., respetando los siguientes criterios:

a) Cada uno de los roles tiene un titular asignado y un sustituto.

b) Los roles son asignados a personal que cumple funciones en ENCODE S.A., excepto en el caso las Autoridades de Registro Delegadas, en este caso será personal propio de las Organizaciones que han convenido con ENCODE S.A.

En el caso de las Autoridades de Registro Delegadas, la Autoridad de Registro Central realizará los controles funcionales, verificando el cumplimiento de las responsabilidades y procedimientos de acuerdo con lo establecido en la presente Política y sus documentos complementarios.

Cada rol cuenta con su credencial de identificación y autenticación.

5.3. - Controles de seguridad del personal

Los controles de seguridad del personal que desempeñan los roles en el Certificador, serán los establecidos por ENCODE S.A. e implementados a través de su Responsable de Recursos Humanos. ENCODE S.A. realiza una evaluación anual del desempeño de todo su personal.

En el caso de las Autoridades de Registro Delegadas, será responsabilidad de las Organizaciones mantener actualizado el legajo de antecedentes laborales, calificaciones profesionales, experiencia e idoneidad, para evaluar el desempeño del personal que cumpla funciones como Oficiales de Registro. ENCODE S. A. realizará los controles pertinentes, comunicando a la Organización la realización y resultado de ellos.

Antecedentes laborales, calificaciones, experiencia e idoneidad del personal

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

En el caso de las Autoridades de Registro Delegadas de una Organización, la evaluación de los antecedentes personales y profesionales se llevará a cabo en conjunto entre el Responsable de la Autoridad de Registro Central y el Responsable que designe la Organización.

Entrenamiento y capacitación inicial

ENCODE S. A. realiza cursos de entrenamiento e instrucción en las políticas y procedimientos que conforman los manuales operativos de la Autoridad Certificante

ENCODESIN, como así también ante cambios en la tecnología de firma digital o en las plataformas utilizadas.

Esos cursos de entrenamiento e instrucción serán extensivos a las Autoridades de Registro Delegadas y ENCODE S. A. los coordinará con los Responsables de las Organizaciones.

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, ENCODE S. A. elabora programas de capacitación específicos para todo el personal afectado.

Los cursos de actualización técnica serán extensivos a las Autoridades de Registro Delegadas y ENCODE S. A. los coordinará con los Responsables de las Organizaciones.

La capacitación será realizada al menos una (1) vez al año, siendo evaluado el personal afectado y otorgándose certificación cuando así correspondiere.

Frecuencia de rotación de cargos

No existe rotación entre los distintos cargos del personal de la Autoridad Certificante ENCODESIN

Esto es extensivo a las Autoridades de Registro e incluye a las Autoridades de Registro Delegadas.

Sanciones a aplicar por acciones no autorizadas

En el caso de incumplimientos comprobados del personal de ENCODE S.A. la persona será separada del rol y/ o de ENCODE S.A., dependiendo de la gravedad de la acción realizada.

En el caso de incumplimientos comprobados del personal de Autoridades de Registro Delegadas, los apercibimientos y las sanciones por acciones no autorizadas posibles a aplicar son, entre otras:

- Revocación del Certificado Digital de la Autoridad de Registro.
- Carta al legajo del Oficial de Registro
- Cesación de las funciones de un Oficial de Registro
- Suspensión de un Oficial de Registro
- Suspensión o inhabilitación como Autoridad de Registro.
- Resolución de lo convenido entre ENCODE S. A. y la Organización.

Toda sanción a aplicar se comunicará a los interesados en un plazo no mayor a dos (2) días desde el momento de resolución de su aplicación.

Requisitos para contratación de personal

El personal contratado a los efectos de cumplir acciones en el marco de esta Política de Certificación deberá tener el conocimiento y formación suficiente para el mejor cometido de las funciones asignadas. Para ello, ENCODE S. A. 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.

En el caso de las Autoridades de Registro Delegadas, serán los procesos establecidos por la Organización, los cuales deberán contemplar y respetar los requisitos mínimos del perfil laboral para desempeñar el rol de Responsable de Autoridad de Registro y Oficial de Registro convenidos con ENCODE S. A.

Documentación provista al personal, incluidas tarjetas y otros elementos de identificación personal

ENCODE S.A. provee a su personal toda la documentación necesaria para poder cumplir con sus funciones. Asimismo le provee las credenciales de identificación y autenticación de acuerdo con el rol asignado.

6. - CONTROLES DE SEGURIDAD TECNICA

6.1. - Generación e instalación del par de claves criptográficas

6.1.1. - Generación del par de claves criptográficas

La clave privada de la Autoridad Certificante ENCODESIN es generada en ambientes seguros, por personal autorizado, sobre dispositivos criptográficos homologados FIPS 140-2 Nivel 3.

La Autoridad Certificante ENCODESIN genera sus claves mediante el algoritmo RSA con un tamaño de 4096 bits.

La clave privada de las Autoridades de Registro es generada y almacenada por sus responsables, utilizando un dispositivo criptográfico homologado por ENCODE S.A.

Las Autoridades de Registro generan sus claves mediante el algoritmo RSA con un tamaño mínimo de 1024 bits.

En el caso de los solicitantes y suscriptores, las claves son generadas y almacenadas por ellos mismos mediante el algoritmo RSA con un tamaño mínimo de 1024 bits.

Las personas físicas podrán hacerlo a su elección por "software" o por "hardware". En caso de elección por software las claves deben ser resguardadas con un pin de seguridad para su acceso. En el caso de elección por hardware ,el dispositivo criptográfico deberá ser provisto por el suscriptor y debe estar dentro de los modelos especificados en la lista de los dispositivos homologados por ENCODE S.A.

Las personas jurídicas podrán hacerlo a su elección por "software" o por "hardware" provisto por el suscriptor, sobre dispositivos criptográficos deben utilizar los homologados por ENCODE S.A.

Las claves de los suscriptores que cuenten con dispositivos criptográficos externos removibles deberán estar protegidas por tres factores de seguridad: 1) mediante la posesión del dispositivo por el suscriptor, 2) mediante una contraseña de acceso al dispositivo criptográfico definida por el propio suscriptor, 3) la contraseña de la clave privada definida por el propio suscriptor.

6.1.2. - Entrega de la clave privada al suscriptor

Las claves privadas de los suscriptores y del personal de las autoridades de registro son generadas por ellos mismos durante el proceso de Solicitud de Certificado, absteniéndose ENCODE S.A. de generar, exigir o por cualquier otro medio tomar conocimiento o acceder a los datos de creación de firma.

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

El Solicitante entrega la clave pública a la Autoridad Certificante ENCODESIN durante el proceso de Solicitud de Certificado.

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.

El Solicitante debe probar su identidad y demostrar que la solicitud le pertenece, presentándose a la Autoridad de Registro con la Solicitud en la cual se identifica el resumen criptográfico (huella MD5).

6.1.4. - Disponibilidad de la clave pública del certificador

Los certificados de la "Autoridad Certificante ENCODESIN" 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 en la siguiente dirección:

- http://www.encodeac.com.ar/firma-digital

La verificación de la validez de los certificados de los suscriptores de la presente política, se realiza automáticamente a través del siguiente procedimiento:

a) Verificando la cadena de confianza del certificado del suscriptor, que es una cadena de firmas y de certificados, que se realiza de la siguiente manera:
   - Verificar el certificado con que se firma al certificado del suscriptor: Certificado de la Autoridad Certificante ENCODESIN, y
   - Verificar el certificado con que se firma al certificado de la Autoridad Certificante ENCODESIN: Certificado de la Autoridad Certificante Raíz de la República Argentina.

b) Verificando la vigencia y el estado de los certificados, a través de la consulta a las CRLs emitidas por la Autoridad Certificante ENCODESIN y por la Autoridad Certificante Raíz.

6.1.5. - Tamaño de claves

La Autoridad Certificante ENCODESIN utiliza claves RSA con un tamaño de 4096 bits.

Las Autoridades de Registro utilizan 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 ENCODESIN son generadas por hardware sobre dispositivos criptográficos FIPS 140-2 nivel 3.

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

Las claves de los suscriptores son generadas por software o por hardware a través de dispositivos criptográficos propiedad del suscriptor, que cumplen con las normas FIPS 140-2 nivel 2 y son del modelo especificado en la lista de dispositivos homologados por ENCODE S.A.

En caso de elección por software las claves deben ser resguardadas con un pin de seguridad para su acceso. En el caso de elección por hardware ,el dispositivo criptográfico deberá ser provisto por el suscriptor y debe estar dentro de los modelos especificados en la lista de los dispositivos homologados por ENCODE S.A.

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 firmar digitalmente, respetando el alcance definido en la presente Política de Certificación. Los valores a utilizar son: "Firma Digital y No Repudio".

6.2. - Protección de la clave privada

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

6.2.1. - Estándares para dispositivos criptográficos

J. G. M. PROT. 2119

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

Las claves privadas de las Autoridades de Registro son generadas y almacenadas sobre un dispositivo criptográfico diseñado para tal fin que cumple con las normas FIPS 140-2 nivel 2.

La clave privada del suscriptor persona física es generada y almacenada, a su elección, 1) por "software", o 2) por "hardware" sobre dispositivos criptográficos de propiedad del suscriptor y el modelo del dispositivo debe ser alguno de los especificados en la lista de dispositivos homologados por ENCODE S.A.

La clave privada del suscriptor persona jurídica es generada y almacenada, a su elección, 1) por "software", o 2) por "hardware" sobre dispositivos criptográficos de propiedad del

suscriptor que cumplen con las normas FIPS 140-2 nivel 2 . El modelo del dispositivo debe ser alguno de los especificados en la lista de dispositivos homologados por ENCODE S.A.

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

La clave privada de la Autoridad Certificante es activada exclusivamente en las instalaciones de ENCODE S.A. o en su sitio alternativo de contingencia, dentro del nivel de seguridad asignado a las operaciones críticas de la Autoridad Certificante ENCODESIN. Para su activación deben estar presentes, personal autorizado en un número M (3), de N (10) posibles.

Las Autoridades de Registro y los suscriptores de certificados con dispositivos criptográficos propios tienen acceso a su clave privada personal a través de una contraseña de acceso al dispositivo criptográfico y la contraseña de la clave privada.

6.2.3. - Recuperación de clave privada

En caso de necesidad, la Autoridad Certificante ENCODESIN prevé mecanismos de recuperación de su clave privada a partir de las copias de respaldo. Esta recuperación sólo puede ser realizada por personal autorizado, sobre dispositivos criptográficos seguros de los que dispone ENCODE S.A. y exclusivamente en los niveles de seguridad de la Autoridad Certificante ENCODESIN en su sitio principal o en su sitio alternativo de contingencia.

No se implementan mecanismos de resguardo y recuperación de la clave privada de la Autoridad de Registro, ni de los 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 ENCODESIN son realizadas inmediatamente después de su generación, por personal autorizado de ENCODE S.A. y almacenadas en dispositivos criptográficos seguros homologados FIPS 140-2 nivel 3. Estos dispositivos son resguardados en un lugar de acceso restringido.

No se implementa mecanismos de copias de resguardo de la clave privada de las Autoridades de Registro ni de los suscriptores.

6.2.5. - Archivo de clave privada

Las copias de resguardo de la clave privada de la Autoridad Certificante ENCODESIN son conservadas en lugares seguros, al igual que sus elementos de activación, bajo los niveles de seguridad exigidos por la Decisión Administrativa Nº 6/2007.

No se implementan mecanismos de archivo de copias de resguardo de la clave privada de las Autoridades de Registro ni 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 ENCODESIN están soportadas en dispositivos criptográficos homologados FIPS 140-2 nivel 3.

Las claves privadas de las Autoridades de Registro son generadas y almacenadas en dispositivos criptográficos homologados FIPS 140-2 nivel 2 y no permiten su exportación.

Las claves privadas de los suscriptores que tengan dispositivos criptográficos propios son generadas y almacenadas en esos dispositivos, estarán homologados como FIPS 140-2 nivel 2 y no permiten su exportación.

6.2.7. - Método de activación de claves privadas

Para la activación de la clave privada de la Autoridad Certificante ENCODESIN se aplica el control M de N. Todos los responsables necesarios para la activación deberán identificarse frente al sistema según corresponda al rol asignado y en un orden determinado por medio de distintos mecanismos de autenticación, a saber: llave de seguridad, claves secretas o ambos.

Las Autoridades de Registro y los suscriptores de certificados que usen dispositivos criptográficos tienen acceso a su clave privada personal a través de una contraseña de acceso al dispositivo criptográfico y la contraseña de la clave privada.

J. G. M. PROY. 2119

6.2.8. - Método de desactivación de claves privadas

La desactivación de la clave privada de la Autoridad Certificante ENCODESIN puede realizarse en esta implementación, desactivando la partición que la contiene. Esta tarea requiere seguir un procedimiento de excepción, el que debe estar debidamente autorizado por el Responsable de Firma Digital, quien debe, además, participar en la Ceremonia de desactivación de la clave privada de la AC ENCODESIN.

6.2.9. - Método de destrucción de claves privadas

Una vez finalizada la vida útil de la clave privada de la Autoridad Certificante ENCODESIN, la partición del dispositivo criptográfico contenedor de esa clave privada será borrada e inicializada a cero. Esta tarea se realizará en el Sitio de Máxima Seguridad en una Ceremonia preparada a ese efecto, con personal autorizado y con los procedimientos de seguridad establecidos.

Para el caso de que finalice la vida útil de la clave privada de un Oficial de una Autoridad de Registro o de un suscriptor, por motivo de revocación o expiración del certificado asociado, y sin mediar renovación, deberá ser eliminado el certificado asociado al par de claves correspondiente.

6.3. - Otros aspectos de administración de claves

6.3.1. - Archivo permanente de la clave pública

Los certificados emitidos a Suscriptores y a las Autoridades de Registro, como así también el de la Autoridad Certificante ENCODESIN, son almacenados y publicados bajo un esquema de redundancia y respaldados en forma periódica, esto, sumado a la firma de cada uno de ellos, garantiza su integridad.

Todos los certificados son almacenados en soporte 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

El par de claves criptográficas del certificado de la AC ENCODESIN tiene una validez de diez (10) años.

J. G. M. PROT. 2119

El par de claves criptográficas correspondientes a los certificados emitidos por la Autoridad Certificante ENCODESIN podrán ser utilizadas por su suscriptor únicamente durante el periodo de validez de los certificados. Este período para todos los certificados será de un año.

6.4. - Datos de activación

6.4.1. - Generación e instalación de datos de activación

Los dispositivos criptográficos utilizados por las Autoridades de Registro y los suscriptores que los posean, son inicializados por los suscriptores, en caso de corresponder.

Como paso previo a la generación de la clave privada, las Autoridades de Registro y los suscriptores deberán establecer una clave de seguridad de acceso sobre el dispositivo criptográfico denominado contraseña y al momento de la generación, la contraseña de la clave privada. La contraseña de acceso del dispositivo criptográfico y la contraseña de la clave privada, son conocidas sólo por su titular, ya sea una Autoridad de Registro o un suscriptor, con el propósito de proteger la clave privada e impedir el acceso por parte de terceros, incluida la Autoridad Certificante ENCODESIN.

La generación e instalación de los datos de activación de la clave privada de la AC ENCODESIN se realiza durante la Ceremonia Inicial con la participación de los N posibles testigos del control M de N.-

6.4.2. - Protección de los datos de activación

Las Autoridades de Registro y los Suscriptores son responsables de la custodia de sus respectivos dispositivos criptográficos y de la no divulgación de la contraseña de acceso del dispositivo criptográfico ni de la contraseña de la clave privada.

Ni ENCODE S.A., ni la Autoridad de Registro Central, ni las Autoridades de Registro Delegadas implementan mecanismos de respaldo de las contraseñas de la clave privada ni de la contraseña de acceso del dispositivo criptográfico de Autoridades de Registro ni de Suscriptores.

Los datos de activación de la clave privada de la AC ENCODESIN están protegidos por mecanismos de seguridad implementados en el nivel 6 del Sitio de Máxima Seguridad.

6.4.3. - Otros aspectos referidos a los datos de activación

Es responsabilidad de las Autoridades de Registro y de los Suscriptores, elegir contraseñas para sus claves privadas y contraseñas de acceso del dispositivo criptográfico que:

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

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

J. G. M. PROT. 2119

6.5. - Controles de seguridad informática

6.5.1. - Requisitos técnicos específicos

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

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 se realiza por medio de servidores "firewall" y sus propios mecanismos de control y monitoreo.

b) Separación de funciones y roles críticos

Las principales funciones vinculadas a los procesos de 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 ENCODESIN serán desempeñados por los responsables designados. En caso de ausencia temporaria, el responsable será reemplazado por el correspondiente sustituto designado.

Esto aplica a la Autoridad de Registro delegada de acuerdo con lo convenido entre ENCODE S. A. y la Organización.

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 ENCODE S.A., 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 ENCODESIN 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 ENCODE S. A. 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 confiables para identificación de roles afectados al proceso de certificación.

Existen mecanismos confiables de identificación de roles, en forma redundante, para los que intervienen en el proceso de certificación.

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

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

6.5.2. - Calificaciones de seguridad computacional

Los servidores que conforman la Autoridad Certificante ENCODESIN para Personas Físicas y Jurídicas se encuentran alojados en el "Sitio de Máxima Seguridad" o SMS construido con los estándares requeridos para este tipo de ambientes.

Las certificaciones del módulo criptográfico HSM son las siguientes:

- U/L 1950 & CSA C22.2 y en CSA C22.2
- FCC Part 15 – Clase B
- High Assurance HSM
- Common criteria EAL 4+
- FIPS 140-2 Nivel 3

Aplicación PKI AC ENCODESIN:

El software PKI utilizado por la AC ENCODESIN se basa en los servicios de certificados nativos del producto Microsoft Windows Server, permitiendo a su vez darle soporte documental a todos los circuitos diseñados para implementar la infraestructura de clave pública. Es un software totalmente escalable, modular e integrable, e incluye todas las llamadas a las funciones de Microsoft Windows Server que cuenta con un completo

sistema de seguridad diseñado según las normativas de seguridad ITU: X.509v3, RSA: PKCS 1, 7, 9, 10,12 y IETF: RFC2459, CMC.

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

6.6.1. - Controles de desarrollo de sistemas

Los sistemas informáticos son homologados por personal técnico al momento de su implementación, para asegurar que los programas que se ponen en producción respondan a las características de diseño declaradas por el proveedor y oportunamente aceptadas cuando fueron seleccionados.

ENCODE S. A. ha adoptado el modelo de la organización OWASP (Open Web Application Security Project), como su estándar para la seguridad de los sistemas, que aplica tanto en los desarrollos que realiza como en la homologación del software adquirido y en las adaptaciones y el mantenimiento de aplicaciones.

6.6.2. - Administración de controles y seguridad

ENCODE S.A. mantiene el control de los equipos y de la documentación de la configuración del sistema, registrándose toda modificación o actualización a cualquiera de ellos.

El esquema de seguridad física del SMS de la Autoridad Certificante ENCODESIN previene que terceros no autorizados puedan ingresar indebidamente a sus instalaciones.

El control periódico de integridad del sistema de la Autoridad Certificante ENCODESIN, realizado por el servicio ENCODEMON, advierte sobre cualquier cambio realizado, lo identifica y permite comprobar su validez.

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

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

6.7. - Controles de seguridad de red

ENCODE S. A. posee un sistema de protección integral de sus activos informáticos. La red de la Autoridad Certificante ENCODESIN, está aislada de otras redes y se encuentra delimitada por diversos cortafuegos ("firewalls") que proveen el filtrado de los paquetes de datos.

6.8. - Controles de ingeniería de dispositivos criptográficos

Todas las actualizaciones de "software" o "firmware" de los dispositivos criptográficos utilizados por la Autoridad Certificante ENCODESIN son verificados en un ambiente de prueba independiente y, en caso de ser aprobadas las actualizaciones por el personal técnico de ENCODE S. A., son distribuidas y aplicadas 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 Nº 6/2007 de la JGM.

7.1. - Perfil del certificado

El formato de los certificados digitales emitidos bajo esta política cumple con los requerimientos de la Decisión Administrativa Nº 6/2007 de la Jefatura de Gabinete de Ministros y las especificaciones contenidas en RFC 3739 "Internet X.509 Public Key Infrastructure Qualified Certificates Profile" y RFC 5280 "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile".

Bajo esta Política de Certificación se emitirán 2 tipos de certificados: 1) Para Personas Físicas y 2) Para Personas Jurídicas. Para cada tipo de certificado hay diferentes clases, las que se encuentran descriptas en el punto "1.3.3 Suscriptores" de la presente Política.

7.1.1.- Perfil de los certificados para persona física clase A

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 ENCODESIN para Personas Físicas y Jurídicas
serialNumber	2.5.4.5	CUIT 30-71110353-4
organizationName	2.5.4.10	ENCODE S. A.

Campo	Valor	
stateOrProvinceName	2.5.4.8	Córdoba
countryName	2.5.4.6	AR
Validity	*< Validez (desde, hasta)>*	
notBefore	*<fecha, hora, minutos y segundos de emisión>*	
tAfter	*<fecha, hora, minutos y segundos de emisión* + 1 año>	
Subject	*<Nombre distintivo del suscriptor>*	
commonName	2.5.4.3	*<Nombres y Apellidos>*
serialNumber	2.5.4.5	*<Tipo de documento y Numero de Documento>*
title	2.5.4.12	*<Ocupación o actividad por la que requiere el certificado>*
organizationalUnitName	2.5.4.11	*<Certificado Persona fisica de clase A>*
organizationName	2.5.4.10	*< Nombre de la Organización relacionada que lo habilita para ser Suscriptor>*
localityName	2.5.4.7	*<Ciudad en la que trabaja>*
stateOrProvinceName	2.5.4.8	*<Provincia en la que trabaja>*
countryName	2.5.4.6	<Nacionalidad de la Persona Física>
subjectPublicKeyInfo	<clave pública del suscriptor>	
Extensions	<Extensiones del certificado>	
authorityKeyIdentifier	2.5.29.35	<issuer + serialNumber del certificado del emisor>
basicConstraint	2.5.29.19	CA=FALSE PathLenConstraint=Null
keyUsage	2.5.29.15	<usos de claves> Firma digital, Sin repudio
CRLDistributionPoints	2.5.29.31	[1]CRL Distribution Point Distribution Point Name: Full Name: URL= http://www.encodeac.com.ar/crl/encodesin.crl [2]CRL Distribution Point Distribution Point Name: Full Name: URL= http://www.encodesa.com.ar/crl/encodesin.crl

Campo		Valor
CertificatePolicies	2.5.29.32	[1]Certificate Policy: Policy Identifier=<*OID de política asignado por la Autoridad de Aplicación*> [1.1] Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: http://www.encodesa.com.ar/firma-digital/encodesin.pdf userNotice=<Este certificado es emitido por la AC ENCODESIN para Personas Físicas y Jurídicas de ENCODE S.A., Certificador Licenciado en el marco de la Ley Argentina Nº 25.506 de Firma Digital>

7.1.2.- Perfil del certificado para persona física clase B ó C

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 ENCODESIN para Personas Físicas y Jurídicas
serialNumber	2.5.4.5	CUIT 30-71110353-4
organizationName	2.5.4.10	ENCODE S. A.
stateOrProvinceName	2.5.4.8	Córdoba
countryName	2.5.4.6	AR
Validity	<*Validez (desde, hasta)*>	
notBefore	<*fecha, hora, minutos y segundos de emisión*>	
notAfter	<*fecha, hora, minutos y segundos de emisión* + 1 año>	
Subject	<*Nombre distintivo del suscriptor*>	
commonName	2.5.4.3	<*Nombres y Apellidos*>
serialNumber	2.5.4.5	<*Tipo de documento y Numero de Documento*>
title	2.5.4.12	<*Ocupación o actividad por la que requiere el certificado Empleado, contador, asesor legal, otro*>
organizationalUnitName	2.5.4.11	<*Certificado Persona fisica de clase {B ó C}* >

Campo	Valor	
organizationName	2.5.4.10	*< Nombre de la Organización relacionada titular de certificado clase A que lo habilita para ser Suscriptor>*
localityName	2.5.4.7	*<Ciudad en la que trabaja>*
stateOrProvinceName	2.5.4.8	*<Provincia en la que trabaja>*
countryName	2.5.4.6	< Nacionalidad de la persona físisca>
subjectPublicKeyInfo	<clave pública del suscriptor>	
Extensions	<Extensiones del certificado>	
authorityKeyIdentifier	2.5.29.35	<issuer + serialNumber del certificado del emisor>
basicConstraint	2.5.29.19	CA=FALSE PathLenConstraint=Null
keyUsage	2.5.29.15	<usos de claves> Firma digital, Sin repudio
CRLDistributionPoints	2.5.29.31	[1]CRL Distribution Point Distribution Point Name: Full Name: URL= http://www.encodeac.com.ar/crl/encodesin.crl [2]CRL Distribution Point Distribution Point Name: Full Name: URL= http://www.encodesa.com.ar/crl/encodesin.crl
CertificatePolicies	2.5.29.32	[1]Certificate Policy: Policy Identifier=*<OID de política asignado por la Autoridad de Aplicación>* [1.1] Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: http://www.encodesa.com.ar/firma-digital/encodesin.pdf userNotice=<Este certificado es emitido por la AC ENCODESIN para Personas Físicas y Jurídicas de ENCODE S.A., Certificador Licenciado en el marco de la Ley Argentina Nº 25.506 de Firma Digital>

J. G. M. PROY. 2119

7.1.3.- Perfil de los certificados para persona jurídica clase A

Campo	Valor
Version	2

Campo	Valor	
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 ENCODESIN para Personas Físicas y Jurídicas de ENCODE S. A.
serialNumber	2.5.4.5	CUIT 30-71110353-4
organizationName	2.5.4.10	ENCODE S. A.
stateOrProvinceName	2.5.4.8	Córdoba
countryName	2.5.4.6	AR
Validity	*< Validez (desde, hasta)>*	
notBefore	*<fecha, hora, minutos y segundos de emisión>*	
notAfter	*<fecha, hora, minutos y segundos de emisión* + 1 año>	
Subject	*<Nombre distintivo del suscriptor>*	
commonName	2.5.4.3	Unidad Operativa en el suscriptor (Ej., Ger RRHH)
serialNumber	2.5.4.5	<Tipo de documento y Numero de Documento> CUIT + Número de CUIT
organizationalUnitName	2.5.4.11	<Certificado Persona Juridica pública o privada de clase A>
organizationName	2.5.4.10	<Nombre de la persona juridica >
localityName	2.5.4.7	<Ciudad en la que opera la PJ>
stateOrProvinceName	2.5.4.8	<Provincia en la que opera la PJ>
countryName	2.5.4.6	País en que está constituida como Persona Jurídica AR
subjectPublicKeyInfo	<clave pública del suscriptor>	
Extensions	<Extensiones del certificado>	
authorityKeyIdentifier	2.5.29.35	<issuer + serialNumber del certificado del emisor>
basicConstraint	2.5.29.19	CA=FALSE PathLenConstraint=Null
keyUsage	2.5.29.15	<usos de claves> Firma digital, Sin repudio
SubjectAlternativeName		*<Persona fisica titular a cargo de la custodia de la clave>*
commonName	2.5.4.3	*<Nombres y Apellidos>*
serialNumber	2.5.4.5	*<Tipo de documento y Numero de Documento>*
title	2.5.4.12	*<Cargo de la persona titular a cargo de la custodia de la clave>*

Campo	Valor	
CRLDistributionPoints	2.5.29.31	[1]CRL Distribution Point Distribution Point Name: Full Name: URL= http://www.encodeac.com.ar/crl/encodesin.crl [2]CRL Distribution Point Distribution Point Name: Full Name: URL= http://www.encodesa.com.ar/crl/encodesin.crl
CertificatePolicies	2.5.29.32	[1]Certificate Policy: Policy Identifier=*<OID de política asignado por la Autoridad de Aplicación>* [1.1] Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: http://www.encodesa.com.ar/firma-digital/encodesin.pdf userNotice=<Este certificado es emitido por la AC ENCODESIN para Personas Físicas y Jurídicas de ENCODE S. A., Certificador Licenciado en el marco de la Ley Argentina Nº 25.506 de Firma Digital>

7.2. - Perfil de la lista de certificados revocados

Las listas de certificados revocados (CRLs) cumplen con los requerimientos de la Decisión Administrativa 6/2007 de la Jefatura de Gabinete de Ministros y las especificaciones contenidas en el RFC 5280 "*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 ENCODESIN para Personas Físicas y Jurídicas de ENCODE S. A.
serialNumber	2.5.4.5	CUIT 30-71110353-4
organizationName	2.5.4.10	ENCODE S. A.
stateOrProvinceName	2.5.4.8	Córdoba
countryName	2.5.4.6	AR
thisUpdate	*<fecha, hora, minutos y segundos de emisión>*	

Campo	Valor	
nextUpdate	*<fecha, hora, minutos y segundos de próxima emisión>*	
revokedCertificates	*<Certificados Revocados>*	
serialNumber	*<serialNumber del certificado revocado>*	
revocationDate	*<fecha de revocación>*	
extensions	*<Extensiones de la CRL>*	
ReasonCode		*<motivo de revocación del certificado>*
authorityKeyIdentifier	2.5.29.35	*<issuer + serialNumber del certificado del emisor>*
CRLNumber	2.5.29.20	*<Nro. de secuencia de CRL>*

8. - ADMINISTRACION DE ESPECIFICACIONES

8.1. - Procedimientos de cambio de especificaciones

Esta Política de Certificación y sus documentos complementarios serán revisados por ENCODE S.A. en forma periódica para detectar y corregir eventuales faltas de claridad y para adaptarlos a cambios en la normativa.

Todo cambio será sometido a la aprobación de la Autoridad de Aplicación y, una vez aprobado, publicado en el sitio web de ENCODE S.A. y puesto en vigencia.

Cada nueva versión tendrá una descripción de los cambios producidos referidos a la versión previa.

8.2. - Procedimientos de publicación y notificación

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

- http://www.encodeac.com.ar/firma-digital/encodesin.pdf

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

COORDINACIÓN DE DESPACHO Y PROTOCOLIZACIÓN FOLIO Nº 185

Según los establecido por la Ley 25.506 Art. 21 inc. q) y por la Decisión Administrativa Nº 6/2007 de la JGM, la presente política y sus posteriores modificaciones deben ser aprobadas por la Autoridad de Aplicación de Firma Digital de la República Argentina.

J. G. M. PROY. 2119