POLÍTICA ÚNICA DE CERTIFICACIÓN DE DIGILOGIX S.A.

MANUAL DE PROCEDIMIENTOS

(PARTE PÚBLICA)

CERTIFICADOR LICENCIADO

DIGILOGIX S.A.

Versión 1.0 (diciembre 2014)

(Reservado a partir del punto 4.5 inclusive y hasta el final del documento)

ÍNDICE

1- INTRODUCCIÓN.

1.1.- Descripción general

El presente manual describe el conjunto de procedimientos utilizados por el Certificador Licenciado **"DIGILOGIX S.A",** en el cumplimiento de sus responsabilidades de emisión y administración de certificados de clave pública emitidos a favor de sus suscriptores, en el marco de la Ley N° 25.506 de firma digital, su Decreto Reglamentario N° 2628/02 y demás normas aclaratorias y modificatorias.

Este Manual de Procedimientos forma parte de la documentación técnica emitida por la **AC – DIGILOGIX** junto con los siguientes documentos:

a) Política Única de Certificación.
b) Manual de Procedimientos, en sus partes públicas.
c) Plan de Seguridad (integrado por la Política de Seguridad y el Manual de Procedimientos de Seguridad).
d) Plan de Contingencias.
e) Plan de Cese de Actividades..

1.2.- Identificación.

a) Manual de Procedimientos de **DIGILOGIX S.A.** para la digitalización, la gestión administrativa y aduanera, entre otros procesos, para las personas físicas y jurídicas
b) OID de la Política Única de Certificación
c) Versión: 1.0
d) Revisión: Sin revisiones a la fecha de su publicación
e) Lugar o sitio de publicación: se publica en el sitio web de la **AC – DIGILOGIX** (http://www.digilogix.com.ar/documentos/)

1.3.- Participantes y aplicabilidad.

Este Manual de Procedimientos es aplicable a:

a) El Certificador que emite certificados digitales para personas físicas y jurídicas.

b) Las Autoridades de Registro (en adelante AR) que se constituyan en el ámbito de la **"**Política Única de Certificación para la digitalización y la gestión administrativa y aduanera, entre otros procesos, para las personas físicas y jurídicas de **DIGILOGIX S.A"**

c) Los solicitantes y suscriptores de certificados digitales emitidos por el Certificador, en el ámbito de la mencionada Política.

d) Los terceros usuarios que verifican firmas digitales basadas en certificados digitales.

1.3.1.- Certificador.

Los procedimientos descriptos en el presente Manual son de aplicación obligatoria para el Certificador licenciado **DIGILOGIX S.A.**

El Certificador licenciado **DIGILOGIX S.A.** presta los servicios de certificación digital de acuerdo con los términos de la Política Única de Certificación antes mencionada y del presente Manual de Procedimientos de Certificación.

1.3.2.- Autoridad de Registro.

La estructura de las Autoridades de Registro estará conformada de la siguiente manera:

a) Autoridad de Registro Central: se encontrará y operará bajo la órbita directa de **DIGILOGIX S.A**., habilitándose la modalidad itinerante para su funcionamiento y,

b) Autoridades de Registro Descentralizadas: funcionarán en distintas organizaciones previa aprobación, mediante un contrato firmado, previamente firmado entre **DIGILOGIX S.A**. y la organización que constituye la Autoridad de Registro. Estas Autoridades de Registro operarán bajo el estricto control y supervisión de la Autoridad de Registro Central de **DIGILOGIX S.A**.

DIGILOGIX S.A. admite la constitución de Autoridades de Registro externas al ámbito físico donde desarrolla sus actividades, de manera que se encuentren en condiciones de efectuar un adecuado control de identidad de los suscriptores de certificados que les presentaran una solicitud de emisión, dado el tipo de información que manejan y su cercanía al usuario final. En todos los casos, es atribución de la **DIGILOGIX S.A.** autorizar el funcionamiento de las mencionadas Autoridades de Registro descentralizadas.

El contrato a suscribir con las Autoridades de Registro delegadas contendrá como mínimo:

a. Denominación y datos de las partes.
b. Derechos y obligaciones de la Autoridad de Registro Descentralizada Datos de contactos
c. Domicilio en el que la Autoridad de Registro prestará sus servicios
d. Duración del contrato
e. Datos de los firmantes

El contrato deberá ser firmado por las máximas autoridades de **DIGILOGIX S.A**. y la Empresa de la que dependerá la Autoridad de Registro descentralizada correspondiente.
Cada incorporación de una Autoridad de Registro deberá figurar en la Lista correspondiente en el Sitio web del Certificador con los datos completos de contacto y nombre del Responsable.
Lista de Autoridades de Registro: http://www.digilogix.com.ar/ar

1.3.3.- Suscriptores de certificados.

Son las personas físicas y jurídicas titulares de certificados digitales emitidos por el Certificador, en el ámbito de aplicación de esta Política Única de Certificación.

Podrán ser suscriptores de los certificados digitales emitidos por la **AC – DIGILOGIX.**
Las personas físicas y/o jurídicas relacionadas con las funciones de clasificación y/o guarda de documentación pública o privada, procesos de despapelización y/o digitalización y/o desarrollo e implementación de sistemas o aplicativos que protejan la autoría e integridad de la documentación tratada.

a) Las personas físicas y/o jurídicas relacionadas con la gestión administrativa y documental, como ser: recibos de sueldo, correos electrónicos, órdenes de compra, facturas comerciales, documentos laborales, documentos comerciales, contratos, entre otros documentos.

b) Las personas físicas y/o jurídicas vinculadas a cualquier actividad relacionada con funciones de tramitación y administrativas aduaneras.

1.3.4.- Aplicabilidad.

Los certificados digitales emitidos por la Autoridad Certificante de **DIGILOGIX**, en el marco de la presente política, podrán ser utilizados por personas físicas y/o jurídicas para firmar cualquier documento asociado a las obligaciones o relaciones descriptas en el punto 1.3.3.- Suscriptores de certificados y a cualquier otra función propia de **DIGILOGIX S.A**

La presente Política Única de Certificación define dos niveles de seguridad para los certificados emitidos a favor de los suscriptores.

a) Nivel de Seguridad Alto: para los certificados solicitados mediante el uso de dispositivos criptográficos (ejemplo: tokens, smart cards).

b) Nivel de Seguridad Normal: correspondiente a los certificados solicitados y almacenados en un software.

1.4.- Contactos.

Por consultas o sugerencias, por favor dirigirse a:

info@digilogix.com.ar

Personalmente o por correo:

Autoridad Certificante: **AC – DIGILOGIX**
Calle: Rivadavia 789 Piso 4º
Código Postal: 1002
Ciudad Autónoma de Buenos Aires.
TEL: 5917-5890

2. ASPECTOS GENERALES DEL MANUAL DE PROCEDIMIENTOS DE CERTIFICACIÓN.

2.1.- Obligaciones.

2.1.1- Obligaciones del certificador.

En su carácter de Certificador Licenciado **DIGILOGIX S.A.** asume las siguientes obligaciones conforme a la normativa que a continuación se detalle:

a) Informar a quien solicita un certificado con carácter previo a su emisión y utilizando un medio de comunicación las condiciones precisas de utilización del certificado digital, sus características y efectos, la existencia de un sistema de licenciamiento y los procedimientos, forma que garantiza su posible responsabilidad patrimonial y los efectos de la revocación de su propio certificado digital y de la licencia que le otorga el Ente Licenciante.
b) Poner a disposición del solicitante la información indicada, en lenguaje comprensible y de manera que la misma sea libremente accesible y poner a disposición de terceros la parte pertinente de dicha información;
c) 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;
d) Mantener el control exclusivo de sus propios datos de creación de firma digital e impedir su divulgación;
e) Operar utilizando un sistema técnicamente confiable de acuerdo con lo que determine la autoridad de aplicación;
f) Notificar al solicitante las medidas que está obligado a adoptar para crear firmas digitales seguras y para su verificación confiable, y las obligaciones que asume por el solo hecho de ser titular de un certificado digital;
g) Recabar únicamente aquellos datos personales del titular del certificado digital que sean necesarios para su emisión, quedando el solicitante en libertad de proveer información adicional;
h) Mantener la confidencialidad de toda información que no figure en el certificado digital;
i) Poner a disposición del solicitante de un certificado digital toda la información relativa a su tramitación;
j) Mantener la documentación respaldatoria de los certificados digitales emitidos, por DIEZ (10) años a partir de su fecha de vencimiento o revocación;
k) Incorporar en su Política Única de Certificación los efectos de la revocación de su propio certificado digital y/o de la licencia que le otorgara la autoridad de aplicación;
l) 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 versiones de la Política Única de Certificación que hubiere, 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;
m) Publicar en el Boletín Oficial de la REPÚBLICA ARGENTINA aquellos datos que la autoridad de

aplicación determine;

n) Registrar las presentaciones que le sean formuladas, así como el trámite conferido a cada una de ellas;
o) Informar en la Política Única de Certificación que todos los certificados digitales que emiten son personales, es decir, requieren la verificación de la identidad del titular;
p) 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 la Política Única de Certificación y en los certificados digitales;
q) Solicitar inmediatamente al Ente Licenciante 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;
r) Informar inmediatamente al Ente Licenciante sobre cualquier cambio en los datos relativos a su licencia;
s) Permitir el ingreso de los funcionarios autorizados de la autoridad de aplicación, del Ente Licenciante o de los auditores a su local operativo, poner a su disposición toda la información necesaria y proveer la asistencia del caso;
t) 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;
u) Someter a aprobación del Ente Licenciante el Manual de Procedimientos, el Plan de Seguridad y el de Cese de Actividades, así como el detalle de los componentes técnicos a utilizar;
v) Constituir domicilio legal en la REPÚBLICA ARGENTINA;
w) Disponer de recursos humanos y tecnológicos suficientes para operar de acuerdo a las exigencias establecidas en la Ley N° 25.506 y su reglamentación;
x) Cumplir con toda otra obligación emergente de su calidad de titular de la licencia adjudicada por el Ente Licenciante;
y) Comprobar por sí o por medio de una Autoridad de Registro que actúe en nombre y por cuenta suya, la identidad y cualquier otro dato de los solicitantes considerado relevante para los procedimientos de verificación de identidad previos a la emisión del certificado digital, según la Política de Certificación bajo la cual se solicita;
z) Mantener a disposición permanente del público la Política Única de Certificación y el Manual de Procedimientos correspondiente;

aa) Cumplir cabalmente con la Política Única de Certificación acordada con el titular y con su Manual de Procedimientos;

2.1.2.- Obligaciones de la Autoridad de Registro.

Las Autoridades de Registro dependientes de la **AC – DIGILOGIX** asumen las siguientes obligaciones:

a) Recibir las solicitudes de emisión de certificados.
b) Validar la identidad y autenticar los datos de los titulares de certificados.
c) Validar otros datos de los titulares de certificados que se presenten ante ella cuya verificación delegue la **AC – DIGILOGIX**.
d) Remitir las solicitudes aprobadas a la **AC – DIGILOGIX**.
e) Recibir y validar las solicitudes de revocación de certificados que hubieran sido recibidas y aprobadas por ella y direccionar las mismas a la **AC – DIGILOGIX.**
f) Identificar y autenticar los solicitantes de revocación de certificados.
g) Archivar y conservar toda la documentación respaldatoria del proceso de validación de identidad, de acuerdo con los procedimientos establecidos por la **AC – DIGILOGIX.**
h) Cumplir las normas y recaudos establecidos para la protección de datos personales.
i) Cumplir las disposiciones que establezca la Política Única de Certificación y el Manual de Procedimientos de la **AC – DIGILOGIX**, en la parte que resulte aplicable.
j) Proteger su par de claves, de manera que su clave privada se encuentre en todo momento bajo su exclusivo conocimiento y control.

Adicionalmente, las Autoridades de Registro deben:

a) Instruir a sus suscriptores en la tramitación de los servicios provistos por el Certificador y en el manejo de la operatoria de la tecnología de firma
b) Instruir a sus usuarios acerca de las buenas prácticas de utilización de la tecnología de firma digital
c) Asistir a solicitantes o suscriptores en la tramitación de los servicios provistos por el Certificador y en el manejo de la operatoria de la tecnología de firma digital

2.1.3.- Obligaciones del suscriptor del certificado.

El suscriptor de un certificado de clave pública asume las siguientes obligaciones:

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 a la **AC – DIGILOGIX** ante cualquier circunstancia que pueda haber comprometido la privacidad de sus datos de creación de firma;
d) Informar sin demora al certificador licenciado el cambio de alguno de los datos contenidos en el certificado digital que hubiera sido objeto de verificación;
e) Proveer toda la información que le sea requerida a los fines de la emisión del certificado de modo completo y preciso;
f) Utilizar los certificados de acuerdo a los términos y condiciones establecidos en la Política de Certificación que respalde su emisión;
g) Tomar debido conocimiento, a través del procedimiento previsto en cada caso, del contenido de la Política Única de Certificación, del Manual de Procedimientos, del Acuerdo con Suscriptores y de cualquier otro documento aplicable.

2.1.4.- Obligaciones de terceros usuarios.

Sin perjuicio de las responsabilidades que competen al Certificador **DIGILOGIX S.A.** y al suscriptor, los terceros usuarios tienen las siguientes obligaciones:

a) Aceptar los términos de la Política Única de Certificación a través de la aceptación del Acuerdo con terceros usuarios;
b) Rechazar la utilización del certificado para aquellos fines no previstos en la Política Única de Certificación;
c) Verificar el estado de los certificados utilizando la información de estado de revocación adecuada.

2.1.5.- Obligaciones del servicio de repositorio.

El Certificador brinda el servicio de repositorio según lo establecido en el apartado 2.1.5 de la

Política Única de Certificación.

El repositorio de la información exigida será publicada en: http://www.digilogix.com.ar/documentos

2.2.- Responsabilidades.

El Certificador Licenciado **DIGILOGIX S.A.** asume la responsabilidad ante terceros por los incumplimientos de las previsiones de la Ley N° 25.506, el Decreto Reglamentario N° 2628/02 y demás regulaciones aplicables, respecto a los procedimientos que respaldan la emisión de certificados, por los errores u omisiones que presenten los certificados emitidos, por su no revocación en los plazos previstos.

La **DIGILOGIX S.A.** no asume responsabilidad en los casos no establecidos expresamente en la legislación aplicable, en aquellos casos de utilización no autorizada de un certificado cuya descripción se encuentra establecida en la Política Única de Certificación, y en eventuales inexactitudes en los datos contenidos en el certificado que resulten de información facilitada por el titular y que hubiera sido objeto de verificación de acuerdo a los procedimientos establecidos en la Política de Certificación y en el Manual de Procedimientos.

2.3.- Responsabilidad Financiera.

2.3.1.- Responsabilidad Financiera del certificador.

Las responsabilidades financieras se originan en lo establecido por la Ley 25.506 y su Decreto Reglamentario Nº 2628/02 y en las disposiciones de la Política Única de Certificación vinculada a este Manual de Procedimientos.

2.4. - Interpretación y Aplicación de las normas.

2.4.1. - Legislación aplicable.

La interpretación, obligatoriedad, diseño y validez de este documento se encuentra sometido a lo establecido por la Ley Nº 25.506 y su Decreto Reglamentario Nº 2628/02, la Decisión Administrativa N° 927/14 y demás normas complementarias dictadas por la Autoridad de Aplicación.

.

2.4.2.- Forma de interpretación y aplicación.

La interpretación y/o la aplicación del presente Manual de Procedimientos y de cualquiera de sus documentos asociados, será resuelta según las normas mencionadas en el punto anterior y conforme a los procedimientos de resolución de conflictos que se establezcan al efecto.

2.4.3.- Procedimientos de resolución de conflictos.

Si se presentaren conflictos de interpretación de una o más disposiciones relativas a este Manual de Procedimientos, el suscriptor o tercero usuario deberá agotar la vía administrativa con este Certificador. Una vez agotada esta vía, podrá recurrir a la Autoridad de Aplicación.

A los efectos del reclamo antes citado, se procederá de la siguiente manera:

a) Una vez recibido el reclamo en las oficinas del Certificador, este citará al reclamante a una audiencia y labrará un acta que deje expresa constancia de los hechos que motivan el reclamo y de todas y cada uno de los antecedentes que le sirvan de causa.
b) Una vez que el Certificador emita opinión, se notificará al reclamante y se le otorgará un plazo de DIEZ (10) días hábiles administrativos para ofrecer y producir la prueba de su descargo.
c) **DIGILOGIX S.A.** resolverá en un plazo de DIEZ (10) días lo que estime corresponder, conforme a los criterios de máxima razonabilidad, equidad y pleno ajuste al bloque de legalidad vigente y aplicable y notificará su decisión al reclamante.

2.5. – Aranceles

Los certificados digitales emitidos bajo la presente política son expedidos a favor de personas físicas y/o jurídicas a título oneroso, aplicándose aranceles diferenciales asociados a los distintos tipos de certificados.

Los aranceles para las distintas clases de certificados serán publicados en el siguiente sitio web de **DIGILOGIX S.A**.:
http:///www.digilogix.com.ar/suscriptor

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

2.6.1.- Publicación de información del Certificador.

La **AC – DIGILOGIX** mantiene un repositorio en línea de acceso público que contiene:

a) Su certificado digital.
b) La lista de certificados revocados (CRL):
c) La Política de Certificación en su versión vigente y las anteriores si las hubiere.
d) El Manual de Procedimientos en sus aspectos de carácter público, en su versión vigente y las anteriores si las hubiere.
e) El modelo del Acuerdo con Suscriptores.
f) Los Términos y Condiciones con Terceros Usuarios.
g) La Política de Privacidad.
h) Información relevante de los informes de la última auditoría dispuesta por la Autoridad de Aplicación.
i) Datos de contacto de la Autoridad de Aplicación y del Ente Licenciante.

La información precedentemente detallada se encuentra disponible durante las VEINTICUATRO (24) horas los SIETE (7) días de la semana en el siguiente sitio web de **DIGILOGIX S.A:,** http://www.digilogix.com.ar/documentos/

2.6.2.- Frecuencia de publicación.

Producida una actualización de los documentos relacionada con el marco legal u operativo de la **AC – DIGILOGIX**, estos documentos actualizados se publicarán dentro de las VEINTICUATRO (24) horas luego de ser aprobados por el Ente Licenciante.

El repositorio es actualizado inmediatamente después que la información a incluir en el mismo ha sido conocida y verificada por la **AC – DIGILOGIX.**

Asimismo, se emitirá cada VEINTICUATRO (24) horas la Lista de Certificados Revocados (CRL completa). Se emitirán CRL complementarias (delta CRL) con frecuencia horaria.

Los estados de los certificados serán actualizados en el repositorio tan pronto como se hayan cumplido los procedimientos correspondientes establecidos en la Política Única de Certificación y en el presente Manual de Procedimientos para cada caso en particular.

Las emisiones y revocaciones de certificados son incluidas en el repositorio tan pronto como se hayan cumplido los procedimientos de validación de identidad de los solicitantes establecidos en su Política Única de Certificación y en este Manual de Procedimientos para cada caso en particular.

2.6.3.- Controles de acceso a la información.

El repositorio se encuentra disponible para uso público durante VEINTICUATRO (24) horas diarias SIETE (7) días a la semana, sujeto a un razonable calendario de mantenimiento.

La **AC – DIGILOGIX** no establece restricciones al acceso a su Política Única de Certificación, al Acuerdo con Suscriptores, a los Términos y Condiciones con Terceros Usuarios, a este Manual de Procedimientos en sus aspectos de carácter público y a toda otra documentación técnica de carácter.

El Certificador garantiza el acceso a su certificado de clave pública y su estado de validez, a la Lista de Certificados Revocados y sus correspondientes deltas y a la información relevante de los informes de la última auditoría.

2.6.4.- Repositorios de certificados y listas de revocación.

El servicio de repositorio de la **AC – DIGILOGIX** es administrado por **DIGILOGIX S.A.**

El Certificador Licenciado **DIGILOGIX S.A**. provee información del estado de validez de los certificados emitidos por su **AC - DIGILOGIX** por medio de su sitio, http://www.digilogix.com.ar/suscriptor ingresando el número de serie del certificado digital correspondiente, obteniendo la información respecto a su estado.

El repositorio de certificados se actualiza inmediatamente después de ocurrido un cambio en el estado de un certificado digital.

La actualización de la lista de certificados digitales revocados se cumple en forma automática con la correspondiente operación de revocación de la **AC – DIGILOGIX.** Independientemente de ello, la lista se renueva cada VEINTICUATRO (24) horas aunque no hubieran ocurrido novedades.

De este modo, la publicación del estado de los certificados digitales revocados en el sitio web de la **AC – DIGILOGIX** se efectuará de forma inmediata para su consulta por parte de terceros usuarios.

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

El acceso a la lista de certificados revocados es público, no estableciéndose ninguna clase de restricción. Se encuentra disponible en el sitio web de la **AC – DIGILOGIX.**

2.7.- Auditorías.

La **AC – DIGILOGIX** se encuentra sujeta a las auditorías del organismo que sea designado para cumplir dichas funciones de acuerdo a lo establecido en la ley N° 25.506 y su Decreto Reglamentario.

La información relevante de los informes de las auditorías es publicada en el sitio web de la **AC – DIGILOGIX**. https://www.digilogix.com.ar/documentos

Se realiza una auditoría previa al licenciamiento del Certificador a fin de verificar el cumplimiento de los requisitos correspondientes al licenciamiento. Con posterioridad, el Certificador será sujeto a auditorías ordinarias para controlar la continuidad del cumplimiento de las normas vigentes y a auditorías extraordinarias de oficio, según lo disponga la Autoridad de Aplicación.

El Certificador realizará auditorías a sus AR en base a un cronograma anual. Podrá asimismo realizar revisiones ad-hoc cuando las circunstancias lo ameriten. La realización de auditorías periódicas será notificada con al menos CINCO (5) días de anticipación y tendrá como resultado un informe que comprenderá tanto las observaciones encontradas, como un dictamen respecto a la confiabilidad y calidad de la operatoria de la AR y el cumplimiento de las especificaciones de este Manual de Procedimientos y demás documentación aplicable.

El Certificador se reserva el derecho de suspender temporalmente o revocar la autorización para actuar como AR descentralizada, en caso de detectar incumplimientos graves en la operatoria de la AR.

2.8.- Confidencialidad.

2.8.1.- Información confidencial.

Toda información referida a suscriptores que sea recibida en los requerimientos por la **AC – DIGILOGIX** o por sus Autoridades de Registro es confidencial y no puede hacerse pública sin el consentimiento previo de aquellos, salvo que sea requerida judicialmente por juez competente. La exigencia se extiende a toda otra información referida a los suscriptores de certificados a la que tenga acceso la **AC – DIGILOGIX** o sus Autoridades de Registro durante el ciclo de vida del certificado.

Lo indicado no es aplicable cuando se trate de información que se transcriba en el certificado o sea obtenida de fuentes públicas.

DIGILOGIX S.A., en su carácter de Certificador, garantiza la confidencialidad frente a terceros de su clave privada, la que, al ser el punto de máxima confianza, será generada y custodiada conforme a lo que se especifique en la Política Única de Certificación. Asimismo, se considera confidencial cualquier información:

- Resguardada en servidores o bases de datos y vinculada al proceso de gestión del ciclo de vida de los certificados digitales emitidos por el Certificador.
- Almacenada en cualquier soporte, incluyendo aquella que se trasmita verbalmente, vinculada a procedimientos de certificación, excepto aquella declarada como no confidencial en forma expresa.
- Relacionada con los Planes de Contingencia, controles, procedimientos de seguridad y registros de auditoría pertenecientes al Certificador.
- Incluida en Manual de Procedimientos (secciones reservadas), en el Plan de Seguridad y en el Plan de Contingencia de la **AC – DIGILOGIX**.

En todos los caso resulta de aplicación la Ley N° 25.326 de protección de datos personales.

2.8.2.- Información no confidencial.

La siguiente información recibida por la **AC – DIGILOGIX** o por sus Autoridades de Registro no es considerada confidencial:

a) Información incluida en el contenido de los certificados y de las listas de certificados revocados
b) Información sobre personas físicas que se encuentre disponible en certificados o en directorios de acceso público.
c) c) La información incluida en los documentos publicados en el repositorio del Certificador mencionados en el apartado 2.6.1 del presente Manual de Procedimientos.

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

La información referida a la revocación de un certificado no es considerada confidencial. El estado de suspensión de un certificado no es aplicable en el marco de la Ley N° 25.506.

El acceso a las listas de certificados revocados es público y está disponible en el sitio web del Certificador Licenciado **DIGILOGIX S.A** en http://www.digilogix.com.ar/suscriptor

bajo los procedimientos especificados en el punto 2.6.4. – “Repositorios de certificados y listas de revocación” del presente Manual de Procedimientos.

2.8.4.- Divulgación de información a autoridades judiciales.

La información confidencial podrá ser revelada ante un requerimiento judicial emanado de juez competente como parte de un proceso judicial.

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

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

La información confidencial o privada podrá ser revelada ante un requerimiento judicial emanado de juez competente como parte de un proceso judicial o ante requerimiento de autoridad administrativa como parte de un proceso administrativo.

2.8.6.- Divulgación de información por solicitud del suscriptor.

Toda divulgación de información referida a los datos de identificación del suscriptor o a cualquier otra información generada o recibida durante el ciclo de vida del certificado solo podrá efectuarse previa autorización escrita del suscriptor del certificado.

No será necesario el consentimiento cuando:

a) Los datos se hayan obtenido de fuentes de acceso público irrestricto.
b) Los datos se limiten a nombre, documento nacional de identidad, pasaporte, documento de identidad expedido por país miembro del MERCOSUR u ocupación.
c) Aquellos para los que el Certificador hubiera obtenido autorización expresa de su titular.

2.8.7.- -Otras circunstancias de divulgación de información.

Excepto por los casos mencionados en los apartados anteriores, no existen otras circunstancias bajo las cuales pueda divulgarse la información.

2.9. - Derechos de Propiedad Intelectual.

Las aplicaciones y los sistemas informáticos generados por el Certificador con el objeto de desarrollar e implementar la **AC – DIGILOGIX** son propiedad de **DIGILOGIX S.A.**
Los sistemas operativos y de soporte informático no desarrollados por la **AC – DIGILOGIX**, cuentan con su respectiva licencia de uso.

3.- IDENTIFICACIÓN Y AUTENTICACIÓN.

3.1.- Registro inicial.

La **AC – DIGILOGIX** únicamente emite certificados personales, efectuándose una validación personal de la identidad del solicitante, para lo cual se requiere su presencia física ante el responsable de una Autoridad de Registro (central o descentralizada), en el caso de personas físicas. Cuando se trate de personas jurídicas, actuará como solicitante, el representante legal, apoderado, administrador o autoridad competente, según el caso.

A fin de efectuar la validación mencionada, se deben cumplir los siguientes procedimientos:

I. El solicitante efectúa el requerimiento de certificado ingresando al sitio web http://www.digilogix.com.ar/suscriptor
II. Acepta la Política Única de Certificación que respalda la emisión del certificado.
III. Completa el requerimiento de certificado con sus datos personales o los datos correspondientes a la persona jurídica, de ser aplicable, y lo remite vía web a la **AC – DIGILOGIX**.
IV. Se presenta ante la Autoridad de Registro según se establece en el apartado 1.3.2 con la siguiente documentación:

1. Documento Nacional de Identidad (original y fotocopia)
2. Nota de confirmación del requerimiento de certificado firmada por el solicitante.
3. Impresión del número de CUIL/CUIT.
4. Demás documentación exigida en el presente Manual.

La Autoridad de Registro efectúa los siguientes procedimientos:

1) Verifica la recepción de la solicitud vía web
2) Valida la identidad del solicitante, mediante la verificación de su documento de identidad
3) Verifica la titularidad de la solicitud mediante el control de la nota de confirmación del requerimiento.

Efectuados los controles mencionados, el solicitante firma el Acuerdo con Suscriptores, con lo cual acepta las condiciones de emisión y uso del certificado. A continuación la Autoridad de Registro aprueba la solicitud de emisión del certificado. Una vez emitido el certificado, el solicitante recibe vía correo electrónico una notificación en la que se le indica que ha sido emitido, incluyendo las instrucciones para su instalación.

En todos los casos, la **AC – DIGILOGIX** informará a los suscriptores de certificados, con carácter previo a su emisión, acerca de los siguientes aspectos:

I. los procedimientos de verificación utilizados,
II. las condiciones de utilización de los certificados,
III. las obligaciones y responsabilidades de las partes,
IV. la existencia de un sistema de licenciamiento,
V. los efectos de la revocación de su certificado y de la licencia.

Esta información se encuentra disponible en el Acuerdo con Suscriptores publicado en el sitio web de la **AC – DIGILOGIX** y será aceptado por el suscriptor como paso previo al inicio del proceso de emisión del certificado. La **AC – DIGILOGIX** se obliga a cumplir con las disposiciones de la Política Única de Certificación, con su Manual de Procedimientos y con las cláusulas del Acuerdo con Suscriptores.

3.1.1.- Tipos de Nombres.

3.1.2.- Necesidad de Nombres Distintivos.

La **AC – DIGILOGIX** utiliza los siguientes nombres distintivos:

1. “CommonName”: corresponde con el nombre que figura en el documento de identidad del suscriptor o el que surge de la documentación presentada por la persona jurídica, de aplicar

2. “SerialNumber”: contiene el tipo y número de documento del titular o el CUIT de la persona jurídica, de aplicar
3. “OrganizationName”: contienen la información relativa a la Organización u organismo en la que el suscriptor desempeña sus funciones o los datos correspondientes a la persona jurídica, de acuerdo a lo establecido en el apartado 3.1.8. El tipo de asociación entre la organización y el suscriptor es verificado según se establece en el apartado 3.1.9.
4. “LocalityName”: Nombre de la ciudad que surge de la certificación aportada en el proceso de autenticación
5. “StateOrProvinceName”: Nombre de la provincia que surge de la certificación aportada en el proceso de autenticación
6. “CountryName”: representa la nacionalidad de la persona física o el país de domicilio constituido de la persona jurídica.

3.1.3.- Reglas para la interpretación de nombres.

Todos los nombres incluidos en los certificados digitales emitidos bajo la Política Única de Certificación correspondiente a este Manual. coinciden con los consignados en el documento de identidad del suscriptor, o con los que figuran en la documentación presentada por la persona jurídica. Las discrepancias o conflictos que pudieran generarse cuando los datos de los solicitantes o suscriptores contengan caracteres especiales, se tratarán de modo de asegurar la precisión de la información contenida en el certificado digital.

3.1.4.- Unicidad de nombres.

El nombre distintivo es único para cada suscriptor, Podrá existir más de un certificado con igual nombre distintivo, si corresponde al mismo suscriptor.

3.1.5.- Procedimiento de resolución de disputas sobre nombres.

DIGILOGIX S.A. se reserva el derecho de decidir los procedimientos de resolución de los conflictos que pudieran generarse respecto de la utilización de nombres por parte de los suscriptores. En tales casos, corresponde al solicitante del certificado demostrar su interés legítimo y su derecho a

la utilización de un nombre en particular.

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

No aplicable.

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

El solicitante generará su par de claves criptográficas usando su propio equipamiento durante el proceso de solicitud del certificado. Las claves son generadas y almacenadas por el solicitante, no quedando almacenadas la clave privada en el sistema informático del Certificador.

En el caso de solicitudes de certificados de nivel de seguridad Alto, el solicitante genera su par de claves y almacena la clave privada en un dispositivo. Para certificados de nivel de seguridad Normal, el solicitante genera su par de claves y almacena la clave privada vía software en su propio equipo al momento de la solicitud. La aplicación de la **AC – DIGILOGIX** validará el requerimiento del certificado (PKCS#10) con el fin de verificar la posesión de la clave privada por parte del solicitante.

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

Para la solicitud de un certificado de persona jurídica pública o privada, su representante legal, apoderado, administrador o autoridad competente, según sea el caso, completa la solicitud de certificado.

A continuación se presenta ante la AR correspondiente con la siguiente documentación:

a) Documento de identidad (original y fotocopia). De tratarse de argentinos nativos o naturalizados, deberá presentar documento nacional de identidad, libreta cívica o libreta de enrolamiento. Los extranjeros deberán presentar documento nacional de identidad, de poseerlo, o bien pasaporte o documento de identidad del país de origen, cuando fuera aplicable.
b) Nota de confirmación del requerimiento del certificado referida a la persona jurídica solicitante.

c) Acuerdo con Suscriptores firmado
d) Recibo que acredita el pago del certificado correspondiente
e) De tratarse de personas jurídicas privadas, registro con los documentos que se detallan más abajo con copias certificadas por Escribano Público de corresponder:
    a. Estatuto o Contrato Social correspondiente a la Persona Jurídica.
    b. Acta de directorio o Poder General Amplio o Poder Especial que autorice la solicitud de certificado de firma digital
    c. Constancia de inscripción en el Registro Público de Comercio.
    d. Constancia de inscripción en AFIP.
    e. DNI de todos los socios, en caso de sociedades irregulares.

De tratarse de personas jurídicas públicas, deberá presentar nota de la autoridad competente o bien copia certificada del acto administrativo por el cual se le autoriza a efectuar la solicitud del certificado en representación del organismo autorizante.

La Autoridad de Registro verificará la identidad de la persona que se presenta, comprobando asimismo su carácter de representante legal, apoderado, administrador o autoridad competente a través de la verificación de la documentación aportada y si condición de solicitante.

En relación a la modalidad “itinerante”, la Autoridad de Registro Central que concurra a la entidad donde se encuentre el solicitante deberá efectuar las mismas verificaciones indicadas en el presente apartado.

Las Autoridades de Registro conservarán la documentación de respaldo del proceso de verificación de identidad y condición de solicitante, inclusive aquella que no hubiera sido verificada durante este proceso, cumpliéndose las exigencias del artículo 21 inc. f) e i) de la Ley Nº 25.506 y el artículo 34 inc. m) del Decreto Nº 2628/02.

3.1.9.- Autenticación de la identidad de personas físicas.

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

Para la verificación de la identidad requerida en la Política Única de Certificación de la **AC – DIGILOGIX** se establece que la documentación requerida al solicitante de un certificado digital es:

1.- Argentinos nativos o naturalizados: original y fotocopia del documento nacional de identidad, libreta cívica o libreta de enrolamiento.

2.- Extranjeros con residencia en el país -incluida la temporaria o transitoria- presentarán DNI, en caso de poseerlo. De no ser así, presentarán pasaporte o documento de identidad del país de origen, cuando fuera aplicable.

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

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

En relación a la modalidad "itinerante" de funcionamiento, la Autoridad de Registro Central que concurra a la entidad donde se encuentre el solicitante deberá efectuar las mismas verificaciones indicadas en el presente apartado.

Deberá presentar también el comprobante de pago y la documentación que acredite su condición de suscriptor de acuerdo al punto 1.3.3. de la Política Única de Certificación.

Las Autoridades de Registro conservarán la documentación de respaldo del proceso de verificación de identidad, inclusive aquella que no hubiera sido verificada durante este proceso, cumpliéndose las exigencias del artículo 21 inc. f) e i) de la Ley Nº 25.506 y el artículo 34 inc. m) del Decreto Nº 2628/02.

El suscriptor de un certificado firmará su ejemplar del Acuerdo con Suscriptores que, entre otras, contiene la declaración de que la información que presentó para ser incluida en el certificado es correcta.

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

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

3.3.- Generación de nuevo certificado (posterior a revocación).

Los certificados emitidos por la **AC – DIGILOGIX** tienen un período de validez de UN (1) año para las personas físicas desde la fecha de emisión y de TRES (3) años para las personas jurídicas públicas o privadas desde la fecha de emisión.

La **AC – DIGILOGIX** admite la renovación de certificados. A tal fin, la **AC – DIGILOGIX** notificará a los suscriptores con una antelación no menor a QUINCE (15) días acerca de la próxima expiración de su certificado a través de un mensaje de correo electrónico, en el que se le indicará el procedimiento a seguir a efectos de presentar la solicitud de renovación. La solicitud de renovación puede ser efectuada por el suscriptor del certificado dentro de los TREINTA (30) días anteriores a la expiración de su período operacional. La **AC – DIGILOGIX** controla la existencia y validez del certificado, verificando la inexistencia de evidencia sobre el compromiso de la correspondiente clave privada y que la información utilizada para verificar la identidad y atributos del suscriptor es aún válida.

De haberse producido alguna modificación en la información incluida en el certificado que fuera validada al momento de su emisión, la **AC – DIGILOGIX** efectúa una nueva validación a través de la verificación de la documentación respaldatoria, que el suscriptor está obligado a presentar. Los procedimientos a cumplir son similares a los utilizados al momento de la emisión.

En caso de haberse producido modificaciones en los términos y condiciones de la emisión del certificado, las mismas son incluidas en un nuevo Acuerdo con Suscriptores e informadas al suscriptor, quien expresará su aceptación a través de la firma del mencionado Acuerdo.

3.4. - Requerimiento de revocación.

Las solicitudes de revocación de certificados podrán efectuarse por su titular por alguno de los siguientes medios:

a) Por correo electrónico firmado digitalmente a la dirección:
revocacion@digilogix.com.ar
b) Ingresando al sitio web de la **AC – DIGILOGIX** (usando el código de revocación)
www.digilogix.com.ar/suscriptor
c) Personalmente en las oficinas de la **AR** correspondiente.

4.- CICLO DEL CERTIFICADO: REQUERIMIENTOS OPERATIVOS.

4.1.- Solicitud de certificado.

La emisión del certificado a favor de un suscriptor implica su autorización para utilizarlo con los alcances definidos en su Política Única de Certificación y caduca por expiración o revocación del certificado.

Todo suscriptor que se postule para obtener un certificado debe completar un requerimiento, el que estará sujeto a revisión por la Autoridad de Registro, según los procedimientos previstos en los apartados 3.1.8 y 3.1.9.

El proceso de solicitud puede ser iniciado solamente por el interesado o su representante legal, apoderado, administrador o autoridad competente en el caso de la persona física, quien debe acreditar fehacientemente su identidad, a través de la presentación ante la **AC – DIGILOGIX** de la documentación indicada en los apartados 3.1.8 y 3.1.9.

4.2.- - Emisión del certificado.

Una vez finalizado exitosamente el proceso de validación de la identidad del suscriptor según los procedimientos indicados en el apartado 3.1.8 y 3.1.9, se iniciará el proceso de emisión del certificado.

Este comprende los siguientes procedimientos:

a) La Autoridad de Registro accede al sistema, selecciona el requerimiento de certificado, verifica sus atributos con los que figuran en la nota presentada y controla que su código de identificación coincida con el informado. De ser exitosos los controles, ingresa su dispositivo criptográfico de firma a fin de efectuar la aprobación de la solicitud del certificado
b) El solicitante recibirá un mensaje de correo electrónico que le informará acerca de la emisión de su certificado.

4.3.- Aceptación del certificado.

Un certificado emitido por la **AC – DIGILOGIX** se considera aceptado por su titular una vez que este ha firmado el Acuerdo con Suscriptores y dicho certificado sido puesto a su disposición vía correo electrónico para su descarga.

4.4.- Suspensión y Revocación de Certificados.

La **AC – DIGILOGIX** no contempla el estado de suspensión de certificados, en acuerdo a lo dispuesto por la Ley N° 25.506.

4.4.1. - Causas de revocación.

La **AC – DIGILOGIX** revocará los certificados digitales que hubiera emitido en los siguientes casos:

a) A solicitud del titular del certificado.
b) Si determinara que el certificado fue emitido en base a información falsa, que al momento de la emisión hubiera sido objeto de verificación.
c) Si determinara que los procedimientos de emisión y/o verificación han dejado de ser seguros.
d) Por resolución judicial o de la autoridad de aplicación debidamente fundada.
e) Por fallecimiento del titular.
f) Por declaración judicial de ausencia con presunción de fallecimiento del titular.
g) Por declaración judicial de incapacidad del titular.
h) Si se determina que la información contenida en el certificado ha dejado de ser válida.
i) Por el cese de relación de representación respecto de una persona jurídica o si variara su condición de tal.
j) Cuando cese su vínculo laboral con la organización en caso de las personas físicas.
k) Ante incumplimiento por parte del suscriptor de las obligaciones establecidas en el Acuerdo con Suscriptores.
l) Si toma conocimiento de que existe sospecha de que la clave privada del suscriptor se encuentra comprometida.
m) Si la **AC - DIGILOGIX** determina que el certificado no fue emitido de acuerdo a los lineamientos de la Política de Certificación, del Manual de Procedimientos, de la Ley N° 25.506, el Decreto Reglamentario N° 2628/02 y demás normativa sobre firma digital.

En caso que la **AC - DIGILOGIX** determinara que un certificado ha dejado de cumplir con lo dispuesto en la Política Única de Certificación y/o con las normas legales y reglamentarias de la Infraestructura de Firma Digital de la REPÚBLICA ARGENTINA, revocará el mismo en un plazo no superior a las VEINTICUATRO (24) horas de haber efectuado dicha comprobación.

4.4.2. - Autorizados a solicitar la revocación.

Se encuentran autorizados a solicitar la revocación de un certificado emitido por la **AC – DIGILOGIX**:

a) El suscriptor, en caso de personas físicas.
b) El responsable de la **AC – DIGILOGIX.**
c) La Autoridad de Aplicación de la Infraestructura de Firma Digital de la REPÚBLICA ARGENTINA.
d) La autoridad judicial competente.
e) El representante legal de la organización, en caso de personas jurídicas.

4.4.3. - Procedimientos para la solicitud de revocación

a) Recepción e identificación.

Producida una causa de revocación del certificado, el suscriptor del certificado, o bien alguno de los responsables indicados en el apartado 4.4.2 deben comunicarlo a la **AC – DIGILOGIX**. Son aceptados los pedidos de revocación que se efectúen por los siguientes medios:

1. Por correo electrónico firmado digitalmente enviado por el suscriptor o la máxima autoridad de la empresa o entidad, en el caso de personas físicas o por quien acredite representación suficiente, en caso de personas jurídicas
2. Personalmente, presentándose ante la Autoridad de Registro de la **AC – DIGILOGIX,** que corresponda. Si quien concurre es el suscriptor, se dará curso al pedido de revocación en forma inmediata, previa verificación de su documento de identidad. Si quien concurre es un apoderado, representante legal, administrador o autoridad competente, debe acreditar su identidad mediante presentación de su documento de identidad y autorización correspondiente.

3. A través del sitio web de la **AC – DIGILOGIX,** usando el correspondiente código de revocación que le fuera entregado al momento de efectuar la solicitud. La Autoridad de Registro para efectuar la revocación verificará la coincidencia del código mencionado con el que se encuentre registrado en los archivos de la **AC – DIGILOGIX**.

En todos los casos en que se efectúe una revocación se emitirá una nota en la que se individualizará el certificado revocado, incluyendo una breve explicación del motivo que la generara. La nota será firmada y archivada por la Autoridad de Registro. El titular del certificado revocado podrá solicitar una copia de la nota mencionada.

b) Revocación decidida por **DIGILOGIX S.A.** por decisión propia o en virtud de solicitud de autoridad competente

Si **DIGILOGIX S.A.** toma conocimiento, por cualquier medio que fuera, acerca de irregularidades cometidas por el suscriptor de un certificado, las cuales, impliquen un incumplimiento de sus obligaciones descriptas en el apartado 2.1.3 de este Manual, que originen causales de revocación, o en caso de solicitarlo una autoridad competente, debe iniciar de inmediato las verificaciones necesarias a efectos de confirmar dicho incumplimiento. En tal caso, la **AC – DIGILOGIX** procederá a revocar de inmediato el certificado comprometido.

De toda denuncia o notificación que se reciba e investigación que se inicie, así como sus resultados, debe dejarse documentación respaldatoria asentada en archivos que estarán a disposición del Ente Licenciante. Lo mismo debe hacerse con los incumplimientos que se detecten y que motiven revocación de certificados.

4.4.4. - Plazo para la solicitud de revocación.

Las solicitudes de revocación deben ser efectuadas en forma inmediata cuando se presente alguna de las circunstancias previstas en el apartado 4.4.1.
La **AC – DIGILOGIX** dispone de un servicio de recepción de solicitudes de revocación que se encuentra disponible en forma permanente SIETE por VEINTICUATRO (7 x 24 horas).
El plazo máximo entre la recepción de la solicitud de revocación y la actualización del estado del certificado, indicando la revocación, es de VEINTICUATRO (24) horas.

4.4.5. - Causas de suspensión.

La **AC – DIGILOGIX** no contempla el estado de suspensión de certificados, en acuerdo a lo dispuesto por la Ley N° 25.506.

4.4.6. - Autorizados a solicitar la suspensión.

No aplicable.

4.4.7. - Procedimientos para la solicitud de suspensión.

No aplicable.

4.4.8. - Límites del periodo de suspensión de un certificado.

No aplicable.

4.4.9. - Frecuencia de emisión de listas de certificados revocados.

La **AC – DIGILOGIX** emite una Lista de Certificados Revocados cada VEINTICUATRO (24) horas.

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

Los terceros usuarios están obligados a validar el estado de los certificados mediante el control de la lista de certificados revocados.

Los suscriptores y terceros usuarios están obligados a confirmar la autenticidad y validez de la lista de certificados revocados mediante la verificación de la firma digital de la **AC – DIGILOGIX** y de su período de validez.

La **AC – DIGILOGIX** garantiza el acceso permanente, eficiente y gratuito de los titulares de certificados y de terceros usuarios al repositorio de certificados.

4.4.11. - Disponibilidad en línea del servicio de revocación y verificación del estado del certificado.

La **AC – DIGILOGIX** posee un servicio en línea de revocación de certificados y de verificación de su estado. Ambos servicios se encuentran disponibles SIETE por VEINTICUATRO (7 x 24) horas, sujetos a un razonable calendario de mantenimiento.

Las características operacionales de ambos servicios se encuentran disponibles en su sitio web.

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.

La **AC – DIGILOGIX** no utiliza otros medios para la divulgación del estado de revocación de los certificados.

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

El suscriptor del certificado es responsable de comunicar de inmediato a la **AC – DIGILOGIX** acerca del compromiso de su clave privada. Una vez recibida la comunicación y efectuada la verificación indicada en el apartado 4.4.3, la **AC – DIGILOGIX** está obligada a revocar el certificado y a actualizar el repositorio en un plazo máximo de VEINTICUATRO (24) horas.