MANUAL DE PROCEDIMIENTOS

POLÍTICA ÚNICA DE CERTIFICACIÓN DE DIGILOGIX S.A.

CERTIFICADOR LICENCIADO

DIGILOGIX S.A.

Versión 2.0

ÍNDICE

1- INTRODUCCIÓN.

1.1.- Descripción general

El presente manual describe el conjunto de procedimientos utilizados por **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, Decreto N° 182/19 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) Plan de Seguridad (integrado por la Política de Seguridad y el Manual de Procedimientos de Seguridad).
c) Plan de Contingencia.
d) Plan de Cese de Actividades.
e) Términos y condiciones con Terceros Usuarios.
f) Acuerdo con Suscriptores.

1.2.- Nombre e identificación del documento

a) Nombre: Manual de Procedimientos de **DIGILOGIX S.A**.
b) OID de la Política Única de Certificación: 2.16.32.1.1.7
c) Versión: 2.0
d) Lugar o sitio de publicación: se publica en el sitio web de la **AC – DIGILOGIX** (http://www.digilogix.com.ar/documentos/)
e) Fecha de aplicación: A partir de su aprobación por el Ente Licenciante
f) Lugar: REPÚBLICA ARGENTINA.

1.3.- Participantes

Este Manual de Procedimientos es aplicable a:

a) **AC – DIGILOGIX** que emite certificados digitales para Persona Humana y Jurídica y otros servicios relacionados con la firma digital.
b) Las Autoridades de Registro (en adelante AR) que se constituyan en el ámbito de la **"**Política Única de Certificación 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 **DIGILOGIX S.A.**

DIGILOGIX S.A. presta los servicios de emisión de certificados digitales de acuerdo con los términos de la Política Única de Certificación antes mencionada y del presente Manual de Procedimientos.

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 fija o móvil.

b) **Autoridades de Registro Descentralizadas:** funcionarán en distintas organizaciones previa aprobación, mediante un contrato 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. Tal como indica la Resolución N° 946/21, **DIGILOGIX S.A.** deberá notificar al Ente Licenciante a través del módulo Trámites a Distancia (TAD) del sistema de Gestión Documental Electrónica – GDE

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

a. Denominación y datos de las partes.
b. Derechos y obligaciones de la Autoridad de Registro Descentralizada
c. Datos de contactos
d. Domicilio en el que la Autoridad de Registro prestará sus servicios
e. Duración del contrato
f. 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, es decir, nombre, dirección y teléfono. Lista de Autoridades de Registro: https://www.digilogix.com.ar/Home/Contact

1.3.3.- Suscriptores de certificados

Podrán ser suscriptores de los certificados digitales emitidos por la AC – DIGILOGIX:

Las personas humanas y/o jurídicas relacionadas con las funciones, entre otras, 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.

Las personas humanas y/o jurídicas relacionadas, entre otras, 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.

Las personas humanas y/o jurídicas vinculadas, entre otras actividades a las relacionadas con funciones de tramitación y administrativas aduaneras.

Certificados para proveedores de servicios en relación a la Firma Digital, conforme a lo dispuesto en la Resolución 946/21 Anexo I Capítulo V art 33.

Certificado para ser usado en relación con el servicio On Line Certificate Status Protocol (en adelante, OCSP) de consulta sobre el estado de un certificado.

1.3.4.- Terceros usuarios

Son Terceros Usuarios de los certificados emitidos bajo la presente Política Única de Certificación, toda persona humana o jurídica que recibe un documento firmado digitalmente y que genera una consulta para verificar la validez del certificado digital correspondiente, de acuerdo a la normativa vigente aplicable a la Firma Digital.

1.4.- Uso de los certificados

Las claves correspondientes a los certificados digitales que se emitan bajo la presente Política Única de Certificación podrán ser utilizadas en forma interoperable en los procesos de Firma Digital de cualquier documento o transacción y para la autenticación o el cifrado.

1.5.- Administración de la Política

1.5.1.- Organización administradora del documento

Es responsable del presente Manual quien ejerza las funciones de Responsable de la AC – DIGILOGIX:

Correo electrónico: info@digilogix.com.ar

Teléfono: +54 11 4345 5150 opción 4 y líneas rotativas

Domicilio: Rivadavia 789 Piso 4º Código Postal: C1002AAF

Ciudad Autónoma de Buenos Aires

Sitio web: https://www.digilogix.com.ar/

1.5.2.- Contacto

El responsable del registro, mantenimiento e interpretación del presente Manual de DIGILOGIX SA es la máxima autoridad del Certificador Licenciado AC – DIGILOGIX:

Correo electrónico: info@digilogix.com.ar

Teléfono: +54 11 4345 5150 opción 4

Domicilio: Rivadavia 789 Piso 4º Código Postal: C1002AAF

Ciudad Autónoma de Buenos Aires

Sitio web: https://www.digilogix.com.ar/

1.5.3.- Procedimiento de aprobación

La Política Única de Certificación y el Manual de Procedimientos se presentan ante el Ente Licenciante durante el proceso de renovación del licenciamiento para su aprobación a través del correspondiente Acto Administrativo.

1.6.- Definiciones y Acrónimos

1.6.1.- Definiciones

- Autoridad de Aplicación: la SECRETARÍA DE INNOVACIÓN PÚBLICA dependiente de JEFATURA DE GABINETE DE MINISTROS es la Autoridad de Aplicación de firma digital en la REPÚBLICA ARGENTINA.
- Autoridad de Registro: es la entidad que tiene a su cargo las funciones de:

- Recepción de las solicitudes de emisión de certificados.
- Validación de la identidad y autenticación de los datos de los titulares de certificados.
- Validación de otros datos de los titulares de certificados que se presenten ante ella cuya verificación delegue el Certificador Licenciado.
- Remisión de las solicitudes aprobadas al Certificador Licenciado con la que se encuentre operativamente vinculada.
- Recepción y validación de las solicitudes de revocación de certificados; y su direccionamiento al Certificador Licenciado con el que se vinculen.
- Identificación y autenticación de los solicitantes de revocación de certificados.
- Archivo y la conservación de toda la documentación respaldatoria del proceso de validación de identidad, de acuerdo con los procedimientos establecidos por el certificador licenciado.
- Cumplimiento de las normas y recaudos establecidos para la protección de datos personales.
- Cumplimiento de las disposiciones que establezca la Política de Certificación y el Manual de Procedimientos del Certificador Licenciado con el que se encuentre vinculada, en la parte que resulte aplicable.
- Cumplimiento con la Resolución N° 116/17, establece la captura de fotografía digital del rostro y la huella dactilar de los solicitantes y suscriptores de firma digital.

Dichas funciones son delegadas por el certificador licenciado. Puede actuar en una instalación fija o en modalidad móvil.

- Certificado Digital: Se entiende por certificado digital al documento digital firmado digitalmente por un certificador, que vincula los datos de verificación de firma a su titular (Artículo 13 de la Ley N° 25.506).
- Certificador Licenciado: Se entiende por certificador licenciado a toda persona de existencia ideal, registro público de contratos u organismo público que expide certificados, presta otros servicios en relación con la firma digital y cuenta con una licencia para ello, otorgada por el ente licenciante. (Artículo 17 de la Ley N° 25.506).
- Certificación digital de fecha y hora: Indicación de la fecha y hora cierta, asignada a un documento o registro electrónico por una tercera parte confiable y firmada digitalmente por ella. Art. 25 del Decreto N° 182/19
- Ente licenciante: SUBSECRETARÍA DE INNOVACIÓN ADMINISTRATIVA dependiente de la SECRETARÍA DE INNOVACIÓN PÚBLICA de la JEFATURA DE GABINETE DE MINISTROS.
- Lista de certificados revocados: Lista de certificados que han sido dejados sin efecto en forma permanente por el Certificador Licenciado, la cual ha sido firmada digitalmente y publicada por el mismo. En inglés: Certificate Revocation List (CRL).
- Manual de Procedimientos: Conjunto de prácticas utilizadas por el certificador licenciado en la emisión y administración de los certificados. En inglés: Certification Practice Statement (CPS).
- Plan de Cese de Actividades: conjunto de actividades a desarrollar por el certificador licenciado en caso de finalizar la prestación de sus servicios.
- Plan de Continuidad de las operaciones: Conjunto de procedimientos a seguir por el certificador licenciado ante situaciones de ocurrencia no previstas que comprometan la continuidad de sus operaciones.
- Plan de Seguridad: Conjunto de políticas, prácticas y procedimientos destinados a la protección de los recursos del certificador licenciado.
- Política de Privacidad: conjunto de declaraciones que el Certificador Licenciado se compromete a cumplir de manera de resguardar los datos de los solicitantes y suscriptores de certificados digitales por él emitidos.
- Suscriptor o Titular de certificado digital: Persona o entidad a cuyo nombre se emite un certificado y que posee una clave privada que se corresponde con la clave pública contenida en el mismo.
- Tercero Usuario: persona humana o jurídica que recibe un documento firmado digitalmente y que genera una consulta para verificar la validez del certificado digital correspondiente.
- Servicio OCSP (Protocolo en línea del estado de un certificado – Online Certificate Status Protocol): Servicio de verificación en línea del estado de los certificados. El OCSP es un método para determinar el estado de revocación de un certificado digital usando otros medios que no sean el uso de Listas de Revocación de Certificados (CRL). El resultado de una consulta a este servicio está firmado por el certificador que brinda el servicio.
- Servicio de Firma Digital con Custodia Centralizada de Clave Criptográfica: Servicio de firma digital que permite tanto su generación como la realización del proceso de firma digital, el que deberá operar utilizando un sistema técnicamente confiable y seguro conforme los lineamientos establecidos en la Ley

N° 25.506 y modificatorias, cumpliendo con las normas de seguridad acordes a estándares internacionales y de auditoría establecidas por la autoridad de aplicación.

1.6.2. – Acrónimos

AC - Autoridad Certificante
ACR-RA- Autoridad Certificante Raíz de la REPÚBLICA ARGENTINA
AR - Autoridad de Registro
CPS - Certification Practice Statement
CRL - Lista de Certificados Revocados (“Certificate Revocation List”)
CUIL - Clave Única de Identificación Laboral
CUIT - Clave Única de Identificación Tributaria
FIPS - Federal Information Processing Standards
IEC - International Electrotechnical Commission
IETF - Internet Engineering Task Force
OCSP - On Line Certificate Status Protocol
OID - Identificador de Objeto (“ObjectIdentifier”)
PKCS#10 - Public-Key Cryptography Standards
RFC - RequestforComments
RSA - Rivest, Shamir y Adleman
SHA - Secure Hash Algorithm
X509 - Estándar UIT-T para infraestructuras de claves públicas

2.- RESPONSABILIDADES VINCULADAS A LA PUBLICACIÓN Y A LOS REPOSITORIOS

2.1.- Repositorios

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

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.**

2.2- Publicación de información del certificador

AC – DIGILOGIX garantiza el acceso a la información actualizada y vigente publicada en su repositorio de los siguientes elementos:

a) Política Única de Certificación anteriores y vigente

b) Acuerdo con Suscriptores

c) Términos y condiciones con terceros usuarios ("*relying sello decomparties*")

d) Política de Privacidad

e) Manual de Procedimientos (parte pública)

f) Información relevante de los informes de su última auditoría

g) Repositorio de certificados revocados

h) Certificados del Certificador Licenciado y acceso al de la Autoridad Certificante Raíz.

i) Consulta de certificados emitidos (indicando su estado). Se pueden consultar en: https://www.digilogix.com.ar/CertificadoSuscriptor/EstadosCertificados

j) Listado de AR. Se puede consultar en: https://www.digilogix.com.ar/Home/Contact

k) La lista de Certificados Revocados (CRL) en: http://www.digilogix.com.ar/ar/digilogix.crl y http://backup.digilogix.com.ar/ar/digilogix.crl

El servicio de repositorio se encuentra disponible para uso público durante las VEINTICUATRO (24) horas los SIETE (7) días de la semana, sujeto a un razonable calendario de mantenimiento, en el sitio web de **AC – DIGILOGIX**.

http://www.digilogix.com.ar/documentos/

AC – DIGILOGIX está obligado a brindar el servicio de repositorio en cumplimiento de lo dispuesto en la Política Única de Certificación.

2.3. - 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.

2.4.- 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 ese 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.

3.- IDENTIFICACIÓN Y AUTENTICACIÓN

La **AC – DIGILOGIX** para emitir los certificados efectúa 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 Humanas. Cuando se trate de Personas Jurídicas, actuará como solicitante, el representante legal, autorizado, apoderado, administrador o autoridad competente, según el caso.

A fin de efectuar la validación mencionada, el solicitante deberá cumplir el siguiente procedimiento:

a) Presentarse ante un oficial de registro con la documentación correspondiente, previo al pago del certificado y solicitud de turno vía telefónica o e-mail.

b) Registrar una fotografía de su rostro y sus huellas dactilares según Resolución 116/2017

c) Firmar el acuerdo con suscriptores delante el oficial de registro, el mismo puede ser descargado previamente por la web o el oficial de registro puede entregarle una copia.

d) Abrir el correo electrónico enviado por la Autoridad de Registro donde se le presentan sus credenciales de acceso a nuestras aplicaciones (Usuario y Contraseña).

e) Ingresar al sitio web de **DIGILOGIX S.A.** https://digilogix.com.ar

f) Iniciar sesión con sus credenciales

g) Dirigirse a la página de descargas del sitio web de **DIGILOGIX S.A.** https://www.digilogix.com.ar/Descargas

h) Descargar e instalar la aplicación para suscriptores. La Autoridad de Registro posee una PC, con la aplicación descargada donde el suscriptor puede realizar el procedimiento.

i) Utilizar la funcionalidad de “Nueva solicitud” de la aplicación para suscriptores

j) Revisar que sus datos sean correctos y enviar la solicitud a la Autoridad de Registro a través de la aplicación. Se genera el par de claves en el dispositivo criptográfico

k) Esperar la aprobación y emisión del certificado.

l) Una vez emitido el certificado, el mismo se descarga a través de la aplicación para suscriptores y se instala en el dispositivo criptográfico.

Como indica el apartado a) se presenta ante la Autoridad de Registro con la siguiente documentación:

Para Personas Jurídicas Públicas o Privadas:

a) Documento de identidad (original y fotocopia) del responsable autorizado.

b) Acuerdo con Suscriptores firmado con lo cual acepta las condiciones de emisión y uso del certificado.

c) Recibo que acredita el pago del certificado correspondiente

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 o documento análogo.

b) Acta de directorio o Poder General Amplio o Carta Poder firmada por máxima autoridad o Poder Especial que autorice la solicitud de certificado de firma digital.

c) Constancia de inscripción en el Registro Público de Comercio o documento análogo.

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.

Además, cuando corresponda se requiere la presentación de nota que incluya nombre de la aplicación, servicio o unidad Operativa responsable.

Para Personas Humanas:

a) De poseer nacionalidad argentina, se requiere Documento Nacional de Identidad.

b) De tratarse de extranjeros, se requiere Documento Nacional de Identidad argentino o Pasaporte válido u otro documento válido aceptado en virtud de acuerdos internacionales.

En todos los casos, **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. 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.- Asignación de nombres de suscriptores

3.1.1.- Tipos de Nombres

3.1.2.- Necesidad de Nombres Distintivos

Para los certificados de los proveedores de servicios de firma digital o de aplicación:

• “commonName” (OID 2.5.4.3: Nombre común): Corresponde al nombre de la aplicación, servicio o de la unidad operativa responsable del servicio.

• “organizationalUnitName” (OID 2.5.4.11: Nombre de la suborganización): Contiene a las unidades operativas relacionadas con el servicio, en caso de existir, pudiendo utilizarse varias instancias de este atributo de ser necesario.

• “organizationName” (OID 2.5.4.10: Nombre de la organización): Esta presente y coincide con el nombre de la Persona Jurídica Pública o Privada responsable del servicio o aplicación.

• “serialNumber” (OID 2.5.4.5: Nro. de serie): Esta presente y contiene el número de identificación de la Persona Jurídica Pública o Privada responsable del servicio o aplicación, expresado como texto y respetando el siguiente formato y codificación: “[código de identificación]” “[nro. de identificación]”.

El valor para el campo [código de identificación] es: “CUIT”: Clave Única de Identificación Tributaria para las Personas Jurídicas argentinas.

• “countryName” (OID 2.5.4.6: Código de país): Esta presente y representa el país de emisión de los certificados, codificado según el estándar [ISO3166] de DOS (2) caracteres.

Para los certificados de Persona Humana:

• “commonName” (OID 2.5.4.3: Nombre común): Esta presente y se corresponde con el nombre que figura en el Documento de Identidad del suscriptor, acorde a lo establecido en el punto 3.2.3.

• “serialNumber” (OID 2.5.4.5: Nro. de serie): Esta presente y contiene el tipo y número de identificación del titular, expresado como texto y respetando el siguiente formato y codificación: “[tipo de documento]” “[nro. de documento]”

Los valores posibles para el campo [tipo de documento] son:

a. En caso de ciudadanos argentinos o residentes: “CUIT/CUIL”: Clave Única de Identificación Tributaria o Laboral.

b. En caso de extranjeros: “PA” [país]: Número de Pasaporte y código de país emisor. El atributo [país] esta codificado según el estándar [ISO3166] de DOS (2) caracteres.

“EX” [país]: Número y tipo de documento extranjero aceptado en virtud de acuerdos internacionales. El atributo [país] esta codificado según el estándar [ISO3166] de DOS (2) caracteres.

• “countryName” (OID 2.5.4.6: Código de país): Esta presente y representa el país de emisión de los certificados, codificado según el estándar [ISO3166] de DOS (2) caracteres.

Para los certificados de Personas Jurídicas Públicas o Privadas:

• “commonName” (OID 2.5.4.3: Nombre común): Coincide con la denominación de la Persona Jurídica Pública o Privada o con el nombre de la unidad operativa responsable del servicio (ej. Gerencia de Compras).

• “organizationalUnitName” (OID 2.5.4.11: Nombre de la sub organización): Contiene las unidades operativas relacionadas con el suscriptor, pudiendo utilizarse varias instancias de este atributo de ser necesario.

“serialNumber” (OID 2.5.4.5: Nro. de serie): Esta presente y contiene el número de identificación de la Persona Jurídica Pública o Privada, expresado como texto y respetando el siguiente formato y codificación: “[código de identificación]” “[nro. de identificación]”.

Los valores posibles para el campo [código de identificación] son:

a.“CUIT”: Clave Única de Identificación Tributaria para las Personas Jurídicas argentinas.
b.“ID” [país]: Número de identificación tributario para Personas Jurídicas extranjeras. El atributo [país] esta codificado según el estándar [ISO3166] de 2 caracteres.

- “countryName” (OID 2.5.4.6: Código de país): Esta presente y representa el país de emisión de los certificados, codificado según el estándar [ISO3166] de 2 caracteres.

Para los Certificados de Autoridad de Sello de Tiempo:

- “commonName” (OID 2.5.4.3: Nombre común): Indica el nombre del servicio.
- “organizationalUnitName” (OID 2.5.4.11: Nombre de la suborganización): Contiene las unidades operativas relacionadas con el suscriptor, pudiendo utilizarse varias instancias de este atributo de ser necesario.
- “organizationName” (OID 2.5.4.10: Nombre de la organización): Coincide con la denominación de la Persona Jurídica Pública o Privada.
- “serialNumber” (OID 2.5.4.5: Nro de serie): Está presente y contiene el número de identificación de la Persona Jurídica Pública o Privada, expresado como texto y respetando el siguiente formato y codificación: “[código de identificación]” “[nro. de identificación]”

Los valores posibles para el campo [código de identificación] son:
a. “CUIT”: Clave Única de Identificación Tributaria para las Personas Jurídicas argentinas.
b. “ID” [país]: Número de identificación tributaria para Personas Jurídicas extranjeras. El atributo [país] DEBE estar codificado según el estándar [ISO 3166] de DOS (2) caracteres.

- “countryName” (OID 2.5.4.6: Códi go de país): Esta presente y representa el país de emisión de los certificados, codificado según el estándar [ISO 3166] de DOS (2) caracteres.

Para los Certificados de Autoridad de Sello de Competencia:

- “commonName” (OID 2.5.4.3: Nombre común): Indica el nombre de la Autoridad de Competencia.
- “organizationalUnitName” (OID 2.5.4.11: Nombre de la suborganización): Contiene las unidades operativas relacionadas con el suscriptor, pudiendo utilizarse varias instancias de este atributo de ser necesario.
- “organizationName” (OID 2.5.4.10: Nombre de la organización): Coincide con la denominación de la Persona Jurídica Pública o Privada.
- “serialNumber” (OID 2.5.4.5: Nro de serie): Esta presente y contiene el número de identificación de la Persona Jurídica Pública o Privada, expresado como texto y respetando el siguiente formato y codificación: “[código de identificación]” “[nro. de identificación]”.

Los valores posibles para el campo [código de identificación] son: “CUIT”: Clave Única de Identificación Tributaria para las Personas Jurídicas argentinas.

- “countryName” (OID 2.5.4.6: Código de país): Esta presente y representa el país de emisión de los certificados, codificado según el estándar [ISO 3166] de DOS (2) caracteres.

3.1.3. - Anonimato o uso de seudónimos

No se emitirán certificados anónimos o cuyo nombre distintivo contenga seudónimo.

3.1.4. - Reglas para la interpretación de nombres

Todos los nombres representados dentro de los certificados emitidos bajo la presente Política coinciden con los correspondientes al documento de identidad del suscriptor o con la documentación presentada por la Persona Jurídica. Las discrepancias o conflictos que puedan generarse si los datos de los solicitantes o suscriptores contienen caracteres especiales, se tratarán de modo de asegurar la precisión de la información contenida en el certificado.

3.1.5. Unicidad de nombres

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 se basa en la utilización del CUIT y/o CUIL, tanto en el caso de personas humanas como jurídicas.

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

No se admite la inclusión de marcas comerciales, marcas de servicios o nombres de fantasía como nombres distintivos en los certificados, excepto en el caso de Personas Jurídicas o aplicaciones, en los que se aceptará en base a la documentación presentada.

AC – DIGILOGIX se reserva 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.

3.2.- Registro inicial

La Autoridad de Registro es quien se ocupa de la identificación de los solicitantes del certificado de firma digital.

AC – DIGILOGIX cumple con la Ley de Firma Digital Nº 25.506 y el art. 21 punto 7 Anexo del reglamentario, Decreto Nº 182/19, relativos a la información a brindar a los solicitantes.

3.2.1 - Métodos para comprobar la titularidad del par de claves

AC – DIGILOGIX comprueba que el solicitante se encuentra en posesión de la clave privada mediante la verificación de la solicitud del certificado digital en formato PKCS#10, el que no incluye dicha clave. Las claves siempre son generadas por el solicitante. En ningún caso **AC – DIGILOGIX ni** sus autoridades de registro podrán tomar conocimiento o acceder bajo ninguna circunstancia a las claves de los solicitantes o titulares de los certificados, conforme el inciso b) del artículo 21 de la Ley N° 25.506.

En los casos en que el solicitante utilizara un servicio de firma digital con custodia centralizada de claves criptográficas, las claves son generadas y utilizadas en un dispositivo criptográfico FIPS 140-2 nivel 3.

3.2.2 - Autenticación de identidad de Personas Jurídicas Públicas o Privadas

En el caso de certificado de Personas Jurídicas el requerimiento debe efectuarse por la persona debidamente autorizada, será la Autoridad de Registro la encargada de verificar la autenticación de la identidad. Será al solicitante a quien se le tome la fotografía del rostro y la huella dactilar a través de un biométrico en concordancia con la Resolución N° 116/17.

La documentación a presentar es la siguiente:

a) Documento de identidad (original y fotocopia) del responsable autorizado.

b) Acuerdo con Suscriptores firmado con lo cual acepta las condiciones de emisión y uso del certificado.

c) Recibo que acredita el pago del certificado correspondiente

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 o documento análogo.

b) Poder General Amplio, Acta de directorio o Poder Especial que autorice la solicitud de certificado de firma digital.

c) Constancia de inscripción en el Registro Público de Comercio o documento análogo.

d) Constancia de inscripción en AFIP.

e) En caso de sociedades irregulares el DNI de todos los socios.

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.

Además, cuando corresponda se requiere la presentación de nota que incluya nombre de la aplicación, servicio o unidad Operativa responsable.

3.2.3 - Autenticación de la identidad de Personas Humanas

En el caso de las Personas Humanas se debe cumplir con la presencia física del solicitante ante la Autoridad de Registro, donde se tomará la captura de la fotografía del rostro y la huella dactilar a través de un dispositivo

biométrico, también deberá firmar el Acuerdo con Suscriptores delante del oficial de registro, que podrá descargarlo de la página o bien podrá ser entregado por el oficial de registro.
La documentación a presentar es la siguiente:

- De poseer nacionalidad argentina, se requiere Documento Nacional de Identidad.
- De tratarse de extranjeros, se requiere Documento Nacional de Identidad argentino o Pasaporte válido u otro documento válido aceptado en virtud de acuerdos internacionales.

En todos los casos, se conservará UNA (1) copia digitalizada de la documentación de respaldo del proceso de autenticación por parte de **AC – DIGILOGIX** o de la Autoridad de Registro operativamente vinculada.

3.2.4 - Información no verificada del suscriptor

Se conserva la información referida al solicitante que no hubiera sido verificada. Adicionalmente, se cumple con lo establecido en el apartado 3 del inciso b) del art. 14 de la Ley N° 25.506.

3.2.5 - Validación de autoridad

AC-DIGILOGIX o la Autoridad de Registro con la que se encuentre operativamente vinculada, verifica la autorización de la Persona Humana que actúa en nombre de la Persona Jurídica para gestionar el certificado correspondiente. Esto es a través de la documentación correspondiente presentada en el momento del registro inicial.

3.2.6- Criterios para interoperabilidad

Los certificados emitidos pueden ser utilizados por sus titulares en forma interoperable para firmar digitalmente cualquier documento o transacción, así como para autenticación o cifrado.

3.3.- Identificación y autenticación para la generación de un nuevo par de claves (Rutina de Re Key)

3.3.1. Renovación con generación de nuevo par de claves

3.3.2- Generación de un certificado con el mismo par de claves

Los certificados emitidos por la **AC – DIGILOGIX** tienen un período de validez de DOS (2) años para la Persona Humana desde la fecha de emisión y de DOS (2) años para la Persona Jurídica 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. 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.

La renovación procede sin la presencia física del suscriptor frente a la Autoridad de Registro, debe remitir el acuerdo con suscriptores firmado con su firma digital.

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** o **info@digilogix.com.ar**

B) Ingresando al sitio web de la AC – DIGILOGIX a la siguiente URL: http://www.digilogix.com.ar/suscriptor, utilizando los datos de acceso que le fuera informado por email al momento de la emisión de su certificado. Una vez que el suscriptor ingresa a su portal con sus datos de acceso debe ingresar a la solapa CERTIFICADOS, verificar sus datos y presionar REVOCAR, establecer el motivo y presionar nuevamente REVOCAR en ese momento se le pide el pin de revocación.

C) Personalmente presentándose a la Autoridad de Registro correspondiente con documento de identidad que permita acreditar su identidad. Adicionalmente en caso de persona jurídica, se requerirá evidencia del vínculo y la capacidad para solicitar la revocación. En la revocación en forma presencial se cumple con la captura de datos biométricos según Resolución 946/21 Anexo II Capítulo VII punto 7 e).

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 cumplir con lo requerido en el punto 3 de este Manual.

4.1.1.- Solicitantes de certificados

Podrán ser suscriptores de los certificados digitales emitidos por la **AC – DIGILOGIX**:

a) Las personas humanas y/o jurídicas relacionadas con las funciones, entre otras, 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.

b) Las personas humanas y/o jurídicas relacionadas, entre otras, 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.

c) Las personas humanas y/o jurídicas vinculadas, entre otras, actividades a las relacionadas con funciones de tramitación y administrativas aduaneras.

d) Certificados para proveedores de servicios en relación a la firma digital, conforme a lo dispuesto en la Resolución 946/21.

e) Certificado para ser usado en relación con el servicio On Line Certificate Status Protocol (en adelante, OCSP) de consulta sobre el estado de un certificado.

En caso de utilizar un servicio de firma digital con custodia centralizada de claves criptográficas, este deberá estar integrado con los servicios de la Autoridad Certificante del Certificador Licenciado, cumpliendo los requisitos de seguridad de la información que permitan resguardar contra la posibilidad de intrusión y uso no autorizado.

4.1.2.- Solicitud de certificado

Las solicitudes sólo podrán ser iniciadas por el solicitante, en el caso de certificados de Persona Humana, por autorizado o el representante legal o apoderado con poder suficiente a dichos efectos, o por el responsable del servicio, aplicación o sitio web, autorizado a tal fin, en el caso de Personas Jurídicas.

Dicho solicitante debe presentar la documentación prevista en los apartados 3.2.2. - Autenticación de la identidad de Personas Jurídicas Públicas o Privadas y 3.2.3. - Autenticación de la identidad de Persona Humana, así como la constancia de C.U.I.T. o C.U.I.L. Deberá también demostrar la pertenencia a la comunidad de suscriptores prevista en el apartado 1.3.3. Suscriptores de certificados.

Cuando el solicitante se trate de Persona Humana o por el autorizado o el representante legal o apoderado en caso de Persona Jurídica, el responsable del servicio, aplicación o sitio web, autorizado a tal fin, debe probar su carácter de suscriptor para esta Política Única de Certificación de acuerdo a lo indicado en el apartado 1.3.3.

El solicitante deberá:

a) Presentarse ante un oficial de registro con la documentación correspondiente

b) Registrar una fotografía de su rostro y su huella dactilar según Resolución N° 116/17

c) Firmar el acuerdo con suscriptores

d) Abrir el correo electrónico enviado por la Autoridad de Registro donde se le presentan sus credenciales de acceso a nuestras aplicaciones (Usuario y Contraseña).

e) Ingresar al sitio web de DIGILOGIX S.A. https://digilogix.com.ar

f) Iniciar sesión con sus credenciales

g) Dirigirse a la página de descargas del sitio web de DIGILOGIX S.A. https://www.digilogix.com.ar/Descargas

h) Descargar e instalar la aplicación para suscriptores

i) Utilizar la funcionalidad de “Nueva solicitud” de la aplicación para suscriptores

j) Revisar que sus datos sean correctos y enviar la solicitud a la Autoridad de Registro a través de la aplicación. Se genera el par de claves en el dispositivo criptográfico

k) Esperar la aprobación y emisión del certificado.

l) Una vez emitido el certificado, el mismo se descarga a través de la aplicación para suscriptores y se instala en el dispositivo criptográfico

En caso de utilizar un servicio de firma digital con custodia centralizada de claves criptográficas, este deberá estar integrado con los servicios de la Autoridad

4.2.- Procesamiento de la solicitud del certificado

En todos los casos, la Autoridad de Registro efectúa los siguientes pasos:

• Valida la identidad del solicitante o su representante autorizado mediante la verificación de la documentación requerida y el cumplimiento de la Resolución N° 116/17, la AR efectúa una captura de fotografía y de la huella dactilar del solicitante del certificado utilizando un dispositivo biométrico.

• Requiere al solicitante o su representante autorizado la firma del Acuerdo con Suscriptores en su presencia con lo que quedan aceptadas las condiciones de emisión y uso del certificado digital.

• Resguarda toda la documentación respaldatoria del proceso de validación por el término de DIEZ (10) años a partir de la fecha de vencimiento o revocación del certificado.

Una vez finalizado exitosamente el proceso de validación de la identidad del suscriptor 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 y 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.- Emisión del certificado

4.3.1.- Proceso de emisión del certificado

AC - DIGILOGIX emitirá el certificado firmándolo digitalmente y lo pondrá a disposición del suscriptor, en la aplicación de suscriptores.

En el mismo sentido, se emitirá un certificado ante una solicitud de renovación.

El suscriptor recibirá un e-mail, a la casilla de correo declarada por al momento de la registración, que su certificado fue emitido con éxito.

4.3.2.- Notificación de emisión

La **AC - DIGILOGIX** emite el certificado firmándolo digitalmente y lo pone a disposición del suscriptor vía web o a través de la aplicación de suscriptor la cual puede descargarse a través de la página web con las credenciales que se le envían por e-mail.

4.4.- 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 ha sido puesto a su disposición. Una vez realizada la emisión se envía un email al suscriptor dando aviso que su certificado fue emitido con éxito.

4.5.- Uso del par de claves y del certificado

4.5.1.- Uso de la clave privada y del certificado por parte del suscriptor

Las características del procedimiento de generación de la clave privada del suscriptor aseguran que la **AC – DIGILOGIX** se abstiene de generar, exigir, acceder o por cualquier otro medio tomar conocimiento de los datos de creación de su firma digital.

La clave pública del suscriptor del certificado es transferida a la **AC – DIGILOGIX** de manera tal que asegure que:

a) No puede ser cambiada durante la transferencia.
b) El remitente posee la clave privada que corresponde a la clave pública transferida.
c) El remitente de la clave pública es el suscriptor del certificado.

El requerimiento de un certificado se emite en formato PKCS#10 o bien en el formato estándar que lo reemplace en el futuro.

Las claves pueden ser generadas a través de un servicio de custodia centralizada de claves criptográficas conforme Resolución N° 86/2020 de la Secretaria de Innovación Pública, en este caso éste deberá estar integrado con los servicios de la Autoridad Certificante del Certificador Licenciado, cumpliendo los requisitos de seguridad de la información que permiten resguardar contra la posibilidad de intrusión y uno no autorizado.

4.5.2.- Uso de la clave pública y del certificado por parte de terceros usuarios

Los Terceros Usuarios deben:

a) Conocer los alcances del presente Manual;
b) Verificar la validez del certificado digital.

4.6.- Renovación del certificado sin generación de un nuevo par de claves

En el caso de certificados digitales de Persona Humana o Jurídica, la renovación en este apartado aplica a la emisión de UN (1) nuevo certificado sin que haya un cambio en la clave pública o en ningún otro dato del suscriptor. La renovación se podrá realizar siempre que el certificado se encuentre vigente.

A los fines de la obtención del certificado, no se exigirá la presencia física del suscriptor, debiendo éste remitir la constancia firmada digitalmente del inicio del trámite de renovación.

En los certificados de aplicaciones, incluyendo los de servidores, se deberá tramitar UN (1) nuevo certificado, según lo indicado en el apartado anterior.

4.7.- Renovación del certificado con generación de un nuevo par de claves

En este caso no se solicita la presencia física del titular del certificado de firma digital para cumplir con el proceso de renovación, se debe presentar documentación en el caso de que se necesite una actualización, y firmar el acuerdo con suscriptor con firma digital.

4.8.- Modificación del certificado

Es una obligación del suscritor notificar a AC – DIGILOGIX en el caso de que exista algún cambio de alguno de los datos que componen el certificado digital.

4.9.- Suspensión y revocación de certificados

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

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.

4.9.1.- Causas de revocación

AC – DIGILOGIX procederá a revocar los certificados digitales que hubiera emitido en los siguientes casos:

- A solicitud del titular del certificado digital o del responsable autorizado para el caso de los certificados de Personas Jurídicas o aplicación
- Si determinara que el certificado fue emitido en base a información falsa, que al momento de la emisión hubiera sido objeto de verificación.
- Si determinara que los procedimientos de emisión y/o verificación han dejado de ser seguros.
- Por Resolución Judicial.
- Por acto administrativo de la Autoridad de Aplicación debidamente fundado.
- Por fallecimiento del titular.
- Por declaración judicial de ausencia con presunción de fallecimiento del titular.
- Por declaración judicial de incapacidad del titular.
- Si se determina que la información contenida en el certificado ha dejado de ser válida.
- Cuando la clave privada asociada al certificado, o el medio en que se encuentre almacenada, se encuentren comprometidos o corran peligro de estarlo.
- Ante incumplimiento por parte del suscriptor de las obligaciones establecidas en el Acuerdo con Suscriptores.

• Si se determina que el certificado no fue emitido de acuerdo a los lineamientos de la Política Única de Certificación, del Manual de Procedimientos, de la Ley N° 25.506, y su modificatoria, sus normas reglamentarias. AC - DIGILOGIX, de corresponder, revocará el certificado en un plazo no superior a las VEINTICUATRO (24) horas de recibido el requerimiento de revocación.

4.9.2.- Autorizados a solicitar la revocación

Según lo establecido en la Resolución N° 946/21 en su Anexo III Se encuentran autorizados para solicitar la revocación de UN (1) certificado emitido por AC-DIGILOGIX:

a) En el caso de los certificados de personas humanas, el suscriptor del certificado.

b) En el caso de los certificados de persona jurídica o de aplicación, el responsable autorizado que efectuara el requerimiento.

c) En el caso de los certificados de persona jurídica o de aplicación, el responsable debidamente autorizado por la Persona Jurídica que brinda el servicio o es titular del certificado o la aplicación.

d) El Certificador o la Autoridad de Registro.

e) El Ente Licenciante.

f) La autoridad judicial.

g) La Autoridad de Aplicación.

4.9.3.- Procedimientos para la solicitud de revocación

AC - DIGILOGIX garantiza que:

a) Se identifica debidamente al solicitante de la revocación según se establece en el apartado 3.4.

b) Las solicitudes de revocación, así como toda acción efectuada por AC - DIGILOGIX o la Autoridad de Registro en el proceso, están documentadas y conservadas en sus archivos.

c) Se documentan y archivan las justificaciones de las revocaciones aprobadas.

d) Una vez efectuada la revocación, se actualiza el estado del certificado en el repositorio y se incluye en la próxima lista de certificados revocados a ser emitida.

e) El suscriptor del certificado revocado es informado del cambio de estado de su certificado.

El suscriptor podrá pedir la revocación de su certificado a través de alguno de los siguientes medios:

1- Por correo electrónico firmado digitalmente a la dirección: revocacion@digilogix.com.ar

2- Ingresando al sitio web de la AC – DIGILOGIX a la siguiente URL: http://www.digilogix.com.ar/suscriptor, utilizando el usuario y contraseña que le fue enviado vía e-mail al momento de la solicitud de su certificado digital. Este sitio se encuentra disponible las VEINTICUATRO (24) horas del día los SIETE (7) días de la semana, durante todo el año.

3- Personalmente presentándose ante la Autoridad de Registro correspondiente con documento de identidad que permita acreditar su identidad. Adicionalmente en caso de Persona Jurídica, se requerirá evidencia del vínculo y la capacidad para solicitar la revocación.

4.9.4.- 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 4.9.1.

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).

4.9.5.- Plazo para el procesamiento de la solicitud de revocación

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.

4.9.6.- 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.

4.9.7.- Frecuencia de emisión de listas de certificados revocados

AC – DIGILOGIX genera y publica una Lista de Certificados Revocados con una frecuencia diaria, con listas complementarias (delta CRL) en modo horario.

4.9.8.- Vigencia de la lista de certificados revocados

La Lista de Certificados Revocados indicará su fecha de efectiva vigencia, así como la fecha de su próxima emisión.

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

AC – DIGILOGIX pone a disposición de los interesados la posibilidad de verificar el estado de un certificado por medio del acceso a la lista de certificados revocados la que se encuentra publicada en:

-http://www.digilogix.com.ar/ar/digilogix.crl

-http://backup.digilogix.com.ar/ar/digilogix.crl

-http://www.digilogix.com.ar/ar/digilogix+.crl

-http://backup.digilogix.com.ar/ar/digilogix+.crl

Y de la certificación en línea (OCSP), el servicio se encuentra disponible SIETE (7) x VEINTICUATRO (24) horas, sujeto a un razonable calendario de mantenimiento, a partir de su sitio web http://ocsp.digilogix.com.ar/ocsp

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

Se utiliza el protocolo OCSP que permite, mediante su consulta, determinar el estado de un certificado digital y es una alternativa al servicio de CRLs, el que también estará disponible. Este servicio es accedido a través del sitio web http://ocsp.digilogix.com.ar/ocsp. La respuesta de la consulta estará firmada con la clave del certificado OCSP correspondiente.

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

La Autoridad Certificante de DIGILOGIX S.A. permite buscar un certificado y consultar su estado a ese instante desde su sitio web

https://www.digilogix.com.ar/CertificadoSuscriptor/EstadosCertificados

Para consumir este servicio el tercero usuario deberá poseer una computadora con conexión a Internet y un navegador web a fin de poder acceder a la web de DIGILOGIX S.A.

4.9.12.- Requisitos específicos para casos de compromiso de claves

En caso de compromiso de su clave privada, el titular del certificado correspondiente se encuentra obligado a comunicar inmediatamente dicha circunstancia al certificador mediante alguno de los mecanismos previstos en el apartado 4.9.3. - Procedimientos para la solicitud de revocación.

4.9.13.- 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.

4.9.14.- Autorizados a solicitar la suspensión

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

4.9.15.- Procedimientos para la solicitud de suspensión

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

4.9.16.- Limites del periodo de suspensión de un certificado

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

4.10.- Estado del certificado

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.

El estado de suspensión no es aceptado por la **AC – DIGILOGIX**. Tenemos dos tipos de estados: Vigente y Revocado.

4.10.1.- Características técnicas

Los servicios disponibles para la verificación del estado de los certificados emitidos por **AC – DIGILOGIX** son:

- CRL, se emite cada VEINTICUATRO (24) horas y delta CRLs en modo horario.
- OCSP, permite verificar si el certificado se encuentra vigente o ha sido revocado.

4.10.2.- Disponibilidad del servicio

Ambos servicios se encuentran disponibles SIETE (7) x VEINTICUATRO (24) horas, sujetos a un razonable calendario de mantenimiento, a partir de su sitio web http://www.digilogix.com.ar/ar/digilogix.crl y http://backup.digilogix.com.ar/ar/digilogix.crl

4.10.3.- Aspectos Operativos

No existen otros aspectos a mencionar.

4.11.- Desvinculación del suscriptor

Una vez expirado el certificado o si este fuera revocado, de no tramitar un nuevo certificado, su titular se considera desvinculado de los servicios **AC – DIGILOGIX.**

De igual forma se producirá la desvinculación, ante el cese de las operaciones **AC – DIGILOGIX.**

4.12.- Recuperación y custodia de claves privadas

En virtud de lo dispuesto en el inciso b) del art. 21 de la Ley N° 25.506, **AC – DIGILOGIX** se obliga a no realizar bajo ninguna circunstancia la recuperación o custodia de claves privadas de los titulares de certificados digitales.

Asimismo, de acuerdo a lo dispuesto en el inciso a) del art. 25 de la ley antes mencionada, el suscriptor de un certificado emitido en el marco de esta Política Única de Certificación se encuentra obligado a mantener el control exclusivo de su clave privada, no compartirla e impedir su divulgación.

5.- CONTROLES DE SEGURIDAD FISICOS, OPERATIVOS Y DE GESTION

La descripción detallada de los procedimientos referidos a los controles de seguridad física, operativos y de gestión se desarrolla en un documento específico denominado Plan de Seguridad.

5.1.- Controles de seguridad física.

La **AC – DIGILOGIX** implementa controles apropiados que restringen el acceso a los equipos, programas y datos utilizados para proveer el servicio de certificación, solamente a personas debidamente autorizadas.

Se implementan procedimientos de control sobre los siguientes aspectos:

a) Construcción y localización de instalaciones.
b) Acceso físico.
c) Energía y aire acondicionado.
d) Exposición al agua.
e) Prevención y protección contra incendios.
f) Medios de almacenamiento.
g) Disposición de material de descarte.
h) Instalaciones de seguridad externas.

El detalle de la implementación de los controles enumerados se encuentra en el Plan de Seguridad.

5.2.- Controles de Gestión

Se establecen procedimientos de control sobre los siguientes temas:

a) Definición de roles confiables.
b) Separación de funciones.
c) Número de personas requeridas por función (titular y sustituto).
d) Identificación y autenticación para cada rol.

Los roles críticos definidos son:

- Responsable de la **AC - DIGILOGIX**: es la máxima autoridad responsable de la AC ante el Ente Licenciante, los Suscriptores y los Terceros Usuarios. En relación a la Política Única de Certificación, implementa las recomendaciones de las auditorías y administra las versiones. En el Plan de Seguridad, reporta de forma fehaciente al Ente Licenciante todos los incidentes que afecten a la seguridad. Autoriza y administra la aplicación del Plan de Contingencia, notificando al Ente Licenciante. Participa en el Plan de Cese de Actividades, notificando al Ente Licenciante.

- **Definidores**: son los responsables encargados de realizar las definiciones relativas a la Política Única de Certificación, operativas, procedimentales, de seguridad física y lógica, planes de contingencia y de cese de actividades.

- **Desarrolladores de software**: es el personal encargado de desarrollar las aplicaciones informáticas que dan soporte a los servicios de la **AC - DIGILOGIX**.

- **Homologadores**: es el personal encargado de evaluar el software desarrollado, previamente a su puesta en producción.

-Administrador de Servidores: es el personal que administra los servidores de la AC (Core y Publicación). Encargado de conexionar y energizar el equipo en su sitio definitivo. Participa en el proceso de inicialización realizando la instalación de software en los servidores y creación en el Sistema Informático de la **AC - DIGILOGIX** la Autoridad de Registro, a los efectos de emitir el primer certificado digital de usuario. Aplica instalaciones o actualizaciones a los servidores y ejecuta rutinas periódicas de control de registro de ejecuciones, a efectos de mantener el equipamiento operativo.

- **Administrador de HSM**: es el personal que administra el dispositivo criptográfico HSM (Hardware Security Module o Módulo de Seguridad por Hardware). Participa en la inicialización del dispositivo, la generación de respaldos y la restauración de los mismos ante contingencias. Es poseedor de la llave azul utilizada para las tareas de administración del HSM. Ejecuta rutinas periódicas de control, a efectos de mantener el equipamiento operativo, y participa en el proceso de cese de actividades de las claves de la AC.

- **Responsable de AR**: es el responsable de elaborar y mantener el plan de implantación y administración de una Autoridad de Registro Central de la AC - DIGILOGIX y del personal afectado. Participa activamente en el proceso de inicio de la AC solicitando el primer certificado que emita. Posee su par de claves generado y almacenado en dispositivos criptográficos certificados bajo normas FIPS 140-2 Nivel 2.
Es el responsable de la operación de la Autoridad de Registro Central de la **AC - DIGILOGIX**, con capacidad de recibir y aprobar solicitudes de certificados digitales. Revoca certificados por presentación personal de su titular o autorizado. Coordina y administra los recursos que le competen.
Su par de claves es generado y almacenado en dispositivos criptográficos certificados bajo normas FIPS 140-2 Nivel 2.
Es responsable de la incorporación y baja de las Autoridades de Registro Descentralizadas con el soporte del responsable de seguridad.
- **Oficial de Registro**: Personal de la Autoridad de Registro Central y Descentralizada con capacidad de recibir y aprobar solicitudes de certificados digitales. Revoca certificados por presentación personal de su titular o autorizado. Interviene en el proceso de emisión de certificado, identificando al solicitante, comprobando las condiciones de suscriptor, atendiendo la solicitud, y aprobando el trámite, de corresponder. Suscribe la documentación respectiva de las solicitudes aprobadas. Su par de claves es generado y almacenado en dispositivos criptográficos certificados bajo normas FIPS 140-2 Nivel 2, el cual es utilizado en el proceso de autorización de solicitudes.

- **Testigos**: Validan las operaciones críticas autorizando la ejecución de las mismas por medio de llaves especiales que obran en su poder, y que conforman el control “M de N” establecido. Participa en la inicialización de los dispositivos, en los procesos de generación de respaldos y de restauración ante contingencias. Participa en el proceso de cese de actividades de las claves de la AC.

- **Responsable de Comunicaciones**: encargado de la administración de las comunicaciones que dan soporte a la infraestructura de firma en la **AC – DIGILOGIX.**

- **Responsable de Seguridad**: encargado de establecer los filtros, restricciones, y controles, que permitan resguardar la información de la **AC - DIGILOGIX**, y del control y asignación de acceso físico a los recintos. Poseedor de la clave del usuario “admin” del HSM. Interviene en el soporte al proceso de habilitación y baja de las Autoridades de Registro Descentralizadas. Poseedor de la llave roja que participa en el proceso de generación y resguardo de los respaldos del HSM. Participa activamente en la ejecución del Plan de Seguridad, de Contingencia y de Cese de Actividades.

- **Administrador de Partición**: personal encargado de la administración de una partición dentro de la **AC – DIGILOGIX**. Interviene en el proceso de inicialización de los dispositivos, participa en el resguardo y en la recuperación de los datos de la partición. Poseedor de la llave negra.

- **Mesa de Ayuda**: personal encargado de las funciones de Mesa de Ayuda, en relación a las gestiones de certificados, temas de Firma Digital en general y/o en particular, atención de consultas de terceros usuarios, recibe y deriva reportes de incidentes. Su par de claves es generado y almacenado en dispositivos criptográficos certificados bajo normas FIPS 140-2 Nivel 2.

- **Auditor**: personal encargado de las funciones de auditoría interna.

5.3.- Controles de seguridad del Personal

DIGILOGIX S.A. sigue una política de administración de personal que provee razonable seguridad acerca de la confiabilidad y competencia del personal para el adecuado cumplimiento de sus funciones.

El personal seleccionado para cumplir las funciones en **DIGILOGIX S.A.** es considerado confiable y sometido a los procesos de investigación de antecedentes laborales. Las designaciones son notificadas por escrito a cada uno de los interesados, quienes dejan constancia escrita de su aceptación.

Se establecen procedimientos de control sobre los siguientes aspectos:

a) Antecedentes laborales, calificaciones, experiencia e idoneidad del personal que desempeña funciones críticas: todo el personal involucrado en la operatoria de la **AC – DIGILOGIX** es sometido a adecuados procesos de investigación que permitan demostrar su confiabilidad y competencia para las funciones a cumplir. Esta investigación es obligatoria como paso previo al inicio de la relación laboral.

b) Antecedentes laborales, calificaciones, experiencia e idoneidad del personal que cumple funciones administrativas, seguridad o de limpieza: el proceso de investigación mencionado está a cargo del área de Recursos Humanos.

c) Entrenamiento y capacitación inicial: se realiza un proceso de capacitación inicial a todo el personal incorporado.

d) Frecuencia de procesos de actualización técnica: se realizan procesos de actualización técnica semestrales.

e) Frecuencia de rotación de cargos. Se establece una frecuencia de rotación entre el titular y el suplente de cada uno de los roles.

f) Sanciones a aplicar por acciones no autorizadas: se aplicarán las sanciones administrativas de acuerdo al régimen disciplinario vigente.

g) Documentación provista al personal: todo el personal de la **AC – DIGILOGIX** tiene acceso a toda la documentación técnica pública que sea emitida y aprobada en respaldo de los procesos de emisión, actualización y revocación de los certificados, así como sobre aspectos funcionales del sistema informático.

5.4.- Procedimientos de auditoría de seguridad

Se mantienen políticas de registro de eventos, cuyos procedimientos detallados son desarrollados en el Manual de Procedimientos. Se cuenta con procedimientos de auditoría de seguridad sobre los siguientes aspectos:

a) Tipo de eventos registrados. Debe respetarse lo establecido en el Anexo II Sección 3 de la Resolución 946/21. - Administración del ciclo de vida de las claves del certificador. Una vez por mes el/los encargados de seguridad, analiza los datos biométricos registrados, como filmaciones, registros de acceso, buscando accesos no programados o fuera horario laboral. Cada 6 meses el jefe de seguridad realiza una inspección visual de los accesos a las cajas seguridad en zona 4, al estado del HSM. - Administración del ciclo de vida de los Certificados. El jefe de seguridad verifica que cada rol tenga acceso a la sección que corresponda, para evitar superposición de roles y así poder mantener el control por oposición en el ciclo de vida de los certificados entre el oficial de registro quien es el responsable de la solicitud de emisión, revocación y renovación de un certificado y quien es el encargado de ingresar a la sección de nivel 3 para la aprobación. - Administración del ciclo de vida de los dispositivos criptográficos. El oficial de registro, documenta el número de serie del dispositivo criptográfico, entregado al suscriptor en el proceso de emisión y renovación del certificado emitido - Solicitud de Certificados. El auditor interno le solicita al oficial de registro la documentación de certificados seleccionados al azar. - Eventos de Seguridad. El jefe de seguridad realiza inspección de los distintos registros, en busca de inconsistencias y anomalías

b) Frecuencia de procesamiento de registros. - Administración del ciclo de vida de las claves del certificador. Mensual - Administración del ciclo de vida de los Certificados. Mensual - Administración del ciclo de vida de los dispositivos criptográficos. Diario - Solicitud de Certificados. Mensual - Eventos de Seguridad. Diario

c) Período de guarda de los registros. Se guarda DIEZ (10) años

d) Medidas de protección de los registros, incluyendo privilegios de acceso. Protección física los registros se encuentran en la zona de seguridad nivel 4 y lógica acceso con datos Biométricos y claves partida

e) Procedimientos de resguardo de los registros. Se replican todos los servidores con su información contra el sitio de contingencia cada 5 minutos.

f) Sistemas de recolección y análisis de registros (internos vs. externos). Cada dispositivo guarda sus eventos de manera local

g) Notificaciones del sistema de recolección y análisis de registros. Si el dispositivo lo permite, se envía un resumen de seguridad una vez al día por mail.

h) Evaluación de vulnerabilidades. Se realiza test de Seguridad una vez al año.

5.5. - Conservación de registros de eventos

Existen procedimientos de conservación y guarda de registros en los siguientes aspectos, que se encuentran detallados en el Manual de Procedimientos:

a) Tipo de registro archivado. Registros Físicos, Registro de Eventos de Windows, Logs en base de datos y archivos de texto.

b) Período de guarda de los registros. Los registros son guardados por 10 años

c) Medidas de protección de los registros archivados, incluyendo privilegios de acceso. Caja de seguridad en nivel 4 y acceso con datos biométricos y contraseña partidas.

d) Procedimientos de resguardo de los registros. Los registros se sincronizan con la infraestructura de contingencia.

e) Requerimientos para los registros de certificados de fecha y hora. No aplica

f) Sistemas de recolección y análisis de registros (internos vs. externos). Se guarda los mails recibidos en contingencia.

g) Procedimientos para obtener y verificar la información archivada. El procedimiento es manual, que se realiza mensualmente

5.6.- Cambio de claves criptográficas

El par de claves de **AC – DIGILOGIX** ha sido generado con motivo del licenciamiento y tiene una vigencia de DIEZ (10) años. Por su parte la licencia tiene una vigencia de CINCO (5) años.

En todos los casos el cambio de claves criptográficas **AC – DIGILOGIX** implica la emisión de un nuevo certificado por parte de la AC Raíz de la República Argentina. Si la clave privada de **AC – DIGILOGIX** se encontrase comprometida, se procederá a la revocación de su certificado y esa clave ya no podrá ser usada en el proceso de emisión de certificados.

AC – DIGILOGIX tomará los recaudos necesarios para efectuar con suficiente antelación la renovación de su licencia y la obtención del certificado, si correspondiese.

5.7.- Plan de respuesta ante incidentes y recuperación ante desastres

Se describen los requerimientos relativos a la recuperación de los recursos de **AC – DIGILOGIX** en caso de falla o desastre. Estos requerimientos serán desarrollados en el Plan de Continuidad de las Operaciones.

Se han desarrollado procedimientos referidos a:

a) Identificación, registro, reporte y gestión de incidentes.

b) Recuperación ante falla inesperada o sospecha de falla de componentes de hardware, software y datos.

c) Recuperación ante compromiso o sospecha de compromiso de la clave privada de **AC – DIGILOGIX.**

d) Continuidad de las operaciones en un entorno seguro luego de desastres.

Los procedimientos cumplen con lo establecido por el Art. 20 del Decreto Nº 182/2019 en lo relativo a los servicios de infraestructura tecnológica prestados por un tercero.

5.8.- Plan de cese de actividades

Se describen los requisitos y procedimientos a ser adoptados en caso de finalización de servicios del certificador o de una o varias de sus autoridades certificantes o de registro. Estos requerimientos son desarrollados en su Plan de Cese de Actividades.

Se han implementado procedimientos referidos a:

a) Notificación al Ente Licenciante, suscriptores, terceros usuarios, otros certificadores y otros usuarios vinculados.

b) Revocación del certificado de **AC – DIGILOGIX** de los certificados emitidos.

c) Transferencia de la custodia de archivos y documentación e identificación de su custodio.

El responsable de la custodia de archivos y documentación cumple con idénticas exigencias de seguridad que las previstas para **AC – DIGILOGIX** o su autoridad certificante o de registro que cesó.

Se contempla lo establecido por el art. 44 de la Ley Nº 25.506 de Firma Digital en lo relativo a las causales de caducidad de la licencia. Asimismo, los procedimientos cumplen lo dispuesto por el art. 20 del Decreto Nº 182/2019, reglamentario de la Ley de Firma Digital, en lo relativo a los servicios de infraestructura tecnológica prestados por un tercero y las obligaciones establecidas en la Resolución N° 946/21 y sus correspondientes Anexos.

6.- CONTROLES DE SEGURIDAD TÉCNICA

DIGILOGIX S.A. define en el Plan Seguridad:

a) Las medidas de seguridad a fin de proteger sus claves criptográficas pública y privada y todos los demás datos críticos necesarios para operar con módulos criptográficos (números pin, contraseñas, etc.).

b) Otros controles de seguridad lógica que garantizan las funciones de generación de claves, identificación de usuarios, emisión y renovación de certificados, auditoría y archivos.

6.1.- Generación e instalación del par de claves criptográficas

La generación e instalación del par de claves es considerada desde la perspectiva de las autoridades certificantes del certificador, de los repositorios, del servicio de custodia centralizada de claves criptográficas, de las autoridades de registro y de los suscriptores. Para cada una de estas entidades se abordan los siguientes temas:

a) Responsables de la generación de claves.

b) Métodos de generación de claves, indicando si se efectúan por software o por hardware.

c) Métodos de entrega y distribución de la clave pública en forma segura.

d) Características y tamaños de las claves.

e) Controles de calidad de los parámetros de generación de claves.

f) Propósitos para los cuales pueden ser utilizadas las claves y restricciones para dicha utilización.

6.1.1.- Generación del par de claves criptográficas

El par de claves del suscriptor de un certificado emitido en los términos de esta Política Única de Certificación es generado y almacenado por el mismo utilizando alguno de los siguientes medios:

• Por software, en este caso, las claves deben ser resguardadas con un PIN de seguridad para su acceso. Conforme al art 5 de la Resolución de la Secretaría de Innovación Pública Nº 86/20 no se permitirá la exportación de estos certificados con su correspondiente clave privada.

• Por hardware, el dispositivo criptográfico deberá ser FIPS 140-2 Nivel 2 o superior.

• A través de un servicio de custodia centralizada de claves criptográficas, conforme Resolución N° 86/20 de la Secretaria de Innovación Pública. Éste deberá estar integrado con los servicios de la Autoridad Certificante del Certificador Licenciado, cumpliendo los requisitos de seguridad de la información que permiten resguardar contra la posibilidad de intrusión y uso no autorizado.

El medio de generación y almacenamiento de la clave privada asegura que:

a) la clave privada es única y su seguridad se encuentra garantizada.

b) no puede ser deducida y se encuentra protegida contra réplicas fraudulentas.

AC – DIGILOGIX luego del otorgamiento de su licencia, genera el par de claves criptográficas en un ambiente seguro con la participación de personal autorizado, sobre dispositivos criptográficos FIPS 140-2 Nivel 3. Para la generación del par de claves, se utilizará el algoritmo RSA de 4096 bits.

En el caso de las Autoridades de Registro, cada Oficial de Registro genera y almacena su par de claves utilizando un dispositivo criptográfico FIPS 140-2 Nivel 2 o superior. Para la generación del par de claves, se utilizará el algoritmo RSA de 2048 bits.

Las claves criptográficas utilizadas por los proveedores de otros servicios relacionados con la firma digital son generadas y almacenadas utilizando dispositivos criptográficos FIPS 140-2 Nivel 2 como mínimo. Para la generación del par de claves, se utilizará el algoritmo RSA de 2048 bits.

6.1.2.- Entrega de la clave privada

Las características del procedimiento de generación de la clave privada del suscriptor aseguran que la **AC – DIGILOGIX** se abstiene de generar, exigir, acceder o por cualquier otro medio tomar conocimiento de los datos de creación de su firma digital.

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

La clave pública del suscriptor del certificado es transferida a la **AC – DIGILOGIX** de manera tal que asegure que:

a) No puede ser cambiada durante la transferencia.

b) El remitente posee la clave privada que corresponde a la clave pública transferida.

c) El remitente de la clave pública es el suscriptor del certificado.

El requerimiento de un certificado se emite en formato PKCS#10 o bien en el formato estándar que lo reemplace en el futuro.

6.1.4. - Disponibilidad de la clave pública del Certificador

El certificado de la **AC – DIGILOGIX** se encuentra a disposición de los suscriptores y terceros usuarios en su sitio web **www.digilogix.com.ar/documentos**

6.1.5. - Tamaño de claves.

AC – DIGILOGIX genera su par de claves criptográficas utilizando el algoritmo RSA de 4096 bits.
Los suscriptores, incluyendo los Oficiales de Registro de las Autoridades de Registro y los Proveedores de otros servicios de firma digital generan sus claves mediante el algoritmo RSA con un tamaño de clave 2048 bits, excepto el caso de las Autoridades de Sello de Tiempo para las que son de 4096 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 las que se señalan en el punto 6.1.5.

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

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

6.2.- Protección de la clave privada y controles sobre los dispositivos criptográficos

La **AC – DIGILOGIX** establece los siguientes procedimientos de control sobre su clave privada:

a) Se establecen dos responsables de su control
b) Se establece un procedimiento de custodia de la clave privada a cargo de ambos responsables.
c) Se establece un procedimiento de activación de la clave privada
d) Se establece un procedimiento de destrucción de la clave privada

Los procedimientos se encuentran detallados en el Plan de Seguridad.

6.2.1.- Controles y estándares para dispositivos criptográficos

Para la generación de claves criptográficas, la **AC – DIGILOGIX** utiliza dispositivos de las siguientes características:

a) Para la generación de las claves criptográficas del certificador: dispositivos certificados NIST de acuerdo a FIPS 140-2 nivel 3.
b) Para la generación de las claves criptográficas utilizadas para la aprobación de las solicitudes de certificados de suscriptores, certificados NIST de acuerdo a FIPS 140-2 nivel 2.

c) Para la generación de las claves criptográficas utilizadas por los suscriptores, dispositivos certificados NIST de acuerdo a FIPS 140-2 nivel 2

d) En el caso del Servicio de Custodia Centralizada de Claves Criptográficas el dispositivo criptográfico de creación de claves del prestador de servicios de confianza debe cumplir con una certificación FIPS 140-2 nivel 3 o superior.

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

El control de la utilización de las claves privadas de la **AC – DIGILOGIX** se encuentra dividido de forma tal que siempre es necesaria la presencia de dos personas distintas para su activación.

6.2.3. - Recuperación de clave privada

La especificación conceptual puede encontrarse en “6.2.3. Recuperación de clave privada” de la Política Única de Certificación de DIGILOGIX S.A.

Para el procedimiento de recuperación de la clave privada de la Autoridad Certificante DIGILOGIX SA se debe disponer de la copia de seguridad (“backup”) en un dispositivo HSM de backup. Se debe tener presente que tanto la obtención de la copia como la recuperación sólo pueden ser realizadas por personal autorizado sobre dispositivos criptográficos seguros, de los que dispone DIGILOGIX S.A., y exclusivamente en los niveles de seguridad de la Autoridad Certificante DIGILOGIX S.A en su sitio principal o en su sitio alternativo de contingencia. El procedimiento en sí mismo es reservado, no es información de divulgación pública.

El resultado del procedimiento es la disponibilidad del servicio de certificación digital, en el sitio principal o en el de contingencia, según como se hubiera requerido.

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

6.2.4. - Copia de seguridad de clave privada

Las copias de la clave privada de la Autoridad Certificante son realizadas inmediatamente después de su generación por personal autorizado y almacenadas en dispositivos criptográficos seguros homologados FIPS 140-2 nivel 3. Estos dispositivos son resguardos en lugar de acceso restringido.

El procedimiento es reservado.

No se implementan mecanismos de copias de resguardo de la clave privada de los Oficiales de Registro y de los suscriptores.

6.2.5. - Archivo de clave privada

Las copias de resguardo de la clave privada de la Autoridad Certificante DIGILOGIX S.A son conservadas en lugares seguros, al igual que sus elementos de activación, bajo los niveles de seguridad requeridos por la normativa vigente. El procedimiento es reservado. No se implementan mecanismos de archivo de copias de resguardo de la clave privada de la Autoridad de Registro y de los suscriptores.

6.2.6.- Transferencias de claves privadas en dispositivos criptográficas

El par de claves criptográficas de la **AC – DIGILOGIX** se genera y almacena en dispositivos criptográficos de acuerdo a lo que se establece en el presente Manual, salvo en el caso de las copias de resguardo que también están soportadas en dispositivos criptográficos homologados FIPS 140-2

nivel 3.

El par de claves criptográficas de las Autoridades de Registro y de los suscriptores de certificados es almacenado en el mismo dispositivo criptográfico FIPS 140-2 nivel 2 donde se genera, no permitiendo su exportación.

6.2.7.- Almacenamiento de caves privadas en dispositivos criptográficas

El almacenamiento de las claves criptográficas del certificador se realiza en el mismo dispositivo de generación que brinda un alto nivel de seguridad de acuerdo a la certificación FIPS 140-2 nivel 3 y en un nivel 6 de seguridad física de acuerdo a lo establecido en el Anexo I Sección 4 de la Resolución N° 946/21.

Las claves criptográficas de las Autoridades de Registro y de los suscriptores de certificados son almacenadas en el mismo dispositivo criptográfico FIPS 140-2 nivel 2 donde se generan, con los mismos niveles de seguridad.

Las claves privadas de los suscriptores que utilizan el Servicio de Custodia Centralizada de Claves Criptográficas son generadas, almacenadas y utilizadas en dispositivos, validados como FIPS 140-2 nivel 3.

6.2.8.- Método de activación de claves privadas

La clave privada de la **AC – DIGILOGIX** se activa previa autenticación de los responsables de su control a través de un procedimiento seguro, establecido en el Plan de Seguridad.

6.2.9.- Método de desactivación de claves privadas

La clave privada de la **AC – DIGILOGIX** se desactiva previa autenticación de los responsables de su control a través de un procedimiento seguro, establecido en el Plan de Seguridad.

6.2.10.- Método de destrucción de claves privadas

En caso de cese de actividades de la **AC – DIGILOGIX** o de compromiso de su clave privada, se destruyen los dispositivos de soporte de su clave privada mediante un procedimiento que garantiza su destrucción total y segura según el último estado del arte disponible a la fecha, detallado en el Plan de Seguridad.

La clave privada de la **AC – DIGILOGIX** empleada para emitir certificados según los lineamientos de este Manual se utiliza únicamente para firmar certificados a favor de suscriptores. Adicionalmente, la mencionada clave sólo puede usarse para firmar listas de certificados revocados.

6.2.11.- Requisitos de los dispositivos criptográficos

La **AC - DIGILOGIX** utiliza un dispositivo criptográfico con la certificación FIPS 140-2 Nivel 3 para la generación y almacenamiento de sus claves.

En el caso de las Autoridades de Registro se utilizan dispositivos criptográficos FIPS 140-2 Nivel 2 o superior.

Los suscriptores utilizan dispositivos criptográficos FIPS 140-2 Nivel 2 o superior.

Los proveedores de otros servicios relacionados con la Firma Digital, utilizan dispositivos FIPS 140-2 Nivel 2 como mínimo.

La capacidad del módulo criptográfico utilizado por el Servicio de Custodia Centralizada de Claves Criptográficas es expresada en cumplimiento como mínimo del estándar FIPS 140-2 nivel 3.

6.3. - Otros aspectos de administración de claves

6.3.1.- Archivo permanente de la clave pública

Se ha definido un procedimiento para el archivo seguro de la clave privada de la **AC – DIGILOGIX**, desarrollado en el Plan de Seguridad.

6.3.2. - Período de uso de clave pública y privada

Las claves privadas correspondientes a los certificados emitidos por la AC – DIGILOGIX pueden ser utilizadas por los suscriptores únicamente durante el período de validez de su certificado.

Las correspondientes claves públicas podrán ser utilizadas durante el período establecido por las normas legales vigentes, a fin de posibilitar la verificación de las firmas generadas durante su período de validez, según se establece en el apartado anterior.

6.4. - Datos de activación

6.4.1. - Generación e instalación de datos de activación

La AC – DIGILOGIX establece medidas adecuadas de seguridad para garantizar que los datos de activación de la clave privada de los suscriptores de certificados sean únicos y aleatorios.

Los datos de activación del dispositivo criptográfico de AC – DIGILOGIX tienen un control “M de N” en base a “M” Poseedores de claves de activación, que deben estar presentes de un total de “N” Poseedores posibles.

Ni AC – DIGILOGIX ni las Autoridades de Registro implementan mecanismos de respaldo de contraseñas y credenciales de acceso a las claves privadas de los suscriptores o Autoridades de Registro o a sus dispositivos criptográficos, si fuera aplicable.

6.4.2. - Protección de los datos de activación

La pérdida, robo o hurto del dispositivo criptográfico de la AC o los del personal afectado a sus funciones, deberá ser denunciada inmediatamente al responsable de seguridad, ya que mientras no se proceda en tal sentido las operaciones registradas durante ese lapso serán responsabilidad del poseedor del mismo.

La pérdida, robo o hurto del dispositivo criptográfico de un suscriptor, implica que el suscriptor o autorizado deban solicitar inmediatamente su revocación a la **AC – DIGILOGIX**.

Cada suscriptor es único responsable por todas las operaciones que queden registradas bajo el dispositivo criptográfico que posee asignado.

Los suscriptores deben colocar una clave de protección del dispositivo criptográfico inmediatamente después de recibirlo y una contraseña de acceso a la clave privada, al generar su par de claves criptográficas.

A efectos de la elección de la clave de protección y de la contraseña de acceso no deben utilizarse combinaciones que sean fácilmente deducibles.

De ningún modo se debe ceder o entregar el dispositivo criptográfico, ni dar a conocer su clave de protección o contraseña de acceso.

Los datos de acceso son tratados como información confidencial y no deben estar expuestos en medios accesibles por terceros.

6.4.3. - Otros aspectos referidos a los datos de activación.

Se establecen medidas adecuadas de seguridad para proteger los datos de activación de las claves, resultando de aplicación los controles establecidos en los apartados 6.1 a 6.3.

6.5.- Controles de seguridad informática

6.5.1. - Requisitos Técnicos específicos.

AC – DIGILOGIX establece requisitos de seguridad referidos al equipamiento y al software de certificación vinculados con los siguientes aspectos:

a) Control de acceso a los servicios y roles afectados al proceso de certificación.

b) Separación de funciones entre los roles afectados al proceso de certificación.

c) Identificación y autenticación de los roles afectados al proceso de certificación.

d) Utilización de criptografía para las sesiones de comunicación y bases de datos.

e) Archivo de datos históricos y de auditoría de **AC – DIGILOGIX** y usuarios.

f) Registro de eventos de seguridad.

g) Prueba de seguridad relativa a servicios de certificación.

h) Mecanismos confiables para identificación de roles afectados al proceso de certificación.

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

Las funcionalidades mencionadas son provistas a través de una combinación del sistema operativo, software de certificación y controles físicos.

6.5.2.- Requisitos de seguridad computacional

Los servidores que conforman la **AC - DIGILOGIX** para Personas Humanas y/o Jurídicas se encuentran alojados en el “Ámbito de Máxima Seguridad” o AMS construido con las certificaciones requeridas para este tipo de ambientes.

Las certificaciones del módulo criptográfico HSM Safenet LUNA SA son las siguientes:

a) U/L 1950 & CSA C22.2 y en CSA C22.2

b) FCC Part 15 – Clase B

c) Keys always in Hardware

d) Luna SA is a High Assurance HSM

e) Common criteria EAL 4+

f) FIPS 140-2 Nivel 3

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

6.6.1. - Controles de desarrollo de sistemas

DIGILOGIX S.A. posee procedimientos para el desarrollo y mantenimiento de la seguridad de sistemas informáticos basados en el modelo OWASP (Open Web Application Security Project) utilizados para el control en la implementación de los sistemas utilizados por la **AC DIGILOGIX.**

6.6.2.- Controles de gestión de seguridad

Se utilizan técnicas de control de integridad para la detección de modificaciones no autorizadas al software o a su configuración.

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

No existen certificaciones de terceros respecto del ciclo de vida del software. (Desarrollo propio)

6.7. - Controles de seguridad de red

Los servicios que provee la **AC – DIGILOGIX** que deban estar conectados a una red de comunicación pública, son protegidos por la tecnología apropiada que garantice su seguridad. Además, se asegura que se exija autorización de acceso a todos los servicios que así lo requieran.

6.8. – Servicios de emisión de sellos de tiempo

El servicio de emisión de sellos de tiempo de la **AC – DIGILOGIX** está basado en la especificación de los estándares

RFC 3161 – “Internet X.509 Public Key Infrastructure Time Stamp Protocol” ; y está sincronizado con la hora oficial de la REPÚBLICA ARGENTINA.

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

7.1. - Perfil del certificado

Todos los certificados son emitidos conforme con lo establecido en la especificación ITU X.509 versión 3, y cumplen con las indicaciones establecidas en la Resolución N° 946/21.

a) Perfil del certificado de Persona Humana

Certificado x.509 v3 Atributos Extensiones	Valor/OID	Contenido
Versión	Version	2 Corresponde a versión 3
Número de serie	SerialNumber 2.5.4.5	Entero positivo asignado unívocamentepor la AC-DIGILOGIX a cada certificado

Algoritmo de Firma	SignatureAlgoritm 2.5.8.3	sha256-RSA 1.2.840.113549.1.1.11
Issuer (Nombre distintivo del emisor)	commonName 2.5.4.3	AC-DIGILOGIX
	serialNumber 2.5.4.5	CUIT 30714128716
	organizationName 2.5.4.10	DIGILOGIX S.A.
	stateOrProvinceName 2.5.4.8	Ciudad Autónoma de Buenos Aires
	countryName 2.5.4.6	AR
Validez (desde, hasta)	notBefore	(Válido desde) <fecha, hora, minutos y segundos deemisión> Fecha y hora en que el período de vigencia del certificado comienza
	notAfter	(Válido hasta) <fecha, hora, minutos y segundos deemisión + 2 años> Fecha y hora en que el periodo de vigencia del certificado termina
Subject (Nombre distintivo del suscriptor)	commonName 2.5.4.3	Nombres y Apellidos
	serialNumber 2.5.4.5	CUIT o CUIL y su número
	countryName 2.5.4.6	Código de País de acuerdo a ISO3166
SubjectPublicKeyInfo (Clave pública del suscriptor)	Publickeyalgorithm	RSA 1.2.840.113549.1.1.1
	Publickeylength	2048 bits Longitud de la clavepública del suscriptor
	Public key	<Clave pública del suscriptor> Valor de la clave pública del suscriptor
Extensiones del certificado (Extensions)		
Restricciones básicas	Basic Constraints 2.5.29.19	Tipo de asunto = Entidad final pathLenghtConstraint = Null

Usos de clave	Key Usage 2.5.29.15	digitalSignature = 1 contentCommitment= 1 keyEncipherment = 1 dataEncipherment = 1 keyAgreement = 0 keyCertSign = 0 cRLSign = 0 encipherOnly = 0 decipherOnly = 0
Identificador de clave del Suscriptor	Subject Key Identifier 2.5.29.14	Contiene un hash de 20bytes del atributo clavepública del suscriptor
Puntos de Distribución de la Lista de Certificados Revocados	CRLDistributionPoints 2.5.29.31	[1]Punto de distribuciónCRL Dirección URL=http://www.digilogix.com.ar/ar/digilogix.crl [2]Punto de distribuciónCRL Dirección URL=http://backup.digilogix.com.ar/ar/digilogix.crl
Política de Certificación	CertificatePolicies 2.5.29.32	OID de la Política de Certificación de DIGILOGIX S.A OID=2.16.32.1.1.7 URL de la Política: https://www.digilogix.com.ar/documentos/cps.pdf Texto de aviso=certificado emitido por un certificador licenciado en el marcode la Ley 25.506
Identificador de la Clave de la Autoridad Certificante	AuthorityKeyIdentifier 2.5.29.35	Contiene un hash de 20bytes del atributo clave pública del DIGILOGIX AC que emitió elcertificado.
Uso Extendido de Clave	Extended Key Usage 2.5.29.37	Autenticación del cliente (1.3.6.1.5.5.7.3.2) Correo seguro (1.3.6.1.5.5.7.3.4) 2.5.29.37
Nombres Alternativos del Suscriptor	SubjectAlternativeName 2.5.29.17	Dirección de mail del suscriptor verificada por circuito seguro compatible con RFC 822

Acceso Información emisor	AuthorityInfoAccess 1.3.6.1.5.5.7.1.1	[1]Authority Info Access Access Method=On- line Certificate Status Protocol (1.3.6.1.5.5.7.48.1) Alternative Name: URL=http://ocsp.digilogix.com.ar/ocsp [2]Authority Info AccessAccess Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2) Alternative Name: URL=http://www.digilogix.com.ar/ar/07.crt
Declaraciones de certificados calificados	QCStatement 1.3.6.1.5.5.7.1.3	OID=2.16.32.1.10.1, cuando las claves sean generadas por software. OID=2.16.32.1.10.2.1, cuando las claves sean generadas en dispositivos que cuenten con certificación FIPS 140 (Versión 2) nivel 1. OID=2.16.32.1.10.2.2, cuando las claves sean generadas en dispositivos que cuenten con certificación FIPS 140 (Versión 2) nivel 2. OID=2.16.32.1.10.2.3, cuando las claves sean generadas en dispositivos que cuenten con certificación FIPS 140 (Versión 2) nivel 3

b) Perfil del certificado de la persona jurídica

Campos Atributos Extensiones	Valor/OID	Contenido
Versión	Version	2 Corresponde a versión 3
Número de serie	SerialNumber 2.5.4.5	Entero positivo asignado unívocamente por la AC-DIGILOGIX a cada certificado
Algoritmo de Firma	SignatureAlgoritm 2.5.8.3	sha256-RSA 1.2.840.113549.1.1.11
	commonName 2.5.4.3	AC-DIGILOGIX
	serialNumber	30714128716

Issuer (Nombre distintivo del emisor)	2.5.4.5	
	organizationName 2.5.4.10	DIGILOGIX S.A.
	stateOrProvinceName 2.5.4.8	Ciudad Autónoma de Buenos Aires
	countryName 2.5.4.6	AR
Validez (desde, hasta)	notBefore	(Válido desde) <fecha,hora, minutos ysegundos de emisión> Fecha y hora en que el período de vigencia del certificado comienza
	notAfter	(Válido hasta) <fecha,hora, minutos y segundos de emisión +2 años> Fecha y hora en que el periodo de vigencia del certificado termina
Subject (Nombre distintivo del suscriptor)	commonName 2.5.4.3	Denominación de la Persona Jurídica
	serialNumber 2.5.4.5	CUIT de la Persona Jurídica
	OrganizationName 2.5.4.10	Nombre de la organización
	organizationalUnitName 2.5.4.11	Nombre de la suborganización
	countryName 2.5.4.6	AR
SubjectPublicKeyInfo (Clave pública del suscriptor)	publickeyalgorithm	RSA 1.2.840.113549.1.1.1
	Publickeylength	2048 bits Longitud de la clave pública del suscriptor
	Public key	< Clave pública del suscriptor> Valor de la clave pública del suscriptor
Extensiones del certificado (Extensions)		
Restricciones básicas	Basic Constraints 2.5.29.19	Tipo de asunto = Entidad final pathLenghtConstraint = Null

Usos de clave	Key Usage 2.5.29.15	digitalSignature = 1 contentCommitment= 1 keyEncipherment = 1 dataEncipherment = 1 keyAgreement = 0 keyCertSign = 0 cRLSign = 0 encipherOnly = 0 decipherOnly = 0
Identificador de clave del Suscriptor	Subject Key Identifier 2.5.29.14	Contiene un hash de 20 bytes del atributo clave pública del suscriptor
Puntos de Distribución de la Lista de Certificados Revocados	CRLDistributionPoints 2.5.29.31	[1] Punto de distribución CRL Dirección URL=http://www.digilogix.com.ar/ar/digilogix.crl [2] Punto de distribución CRL Dirección URL=http://backup.digilogix.com.ar/ar/digilogix.crl
Política de Certificación	CertificatePolicies 2.5.29.32	OID de la Política de Certificación de DIGILOGIX S.A OID=2.16.32.1.1.7 URL de la Política: https://www.digilogix.com.ar/document os/cps.pdf Texto de aviso=certificado emitido por un certificador licenciado en el marco de la Ley 25.506
Identificador de la Clave de la AutoridadCertificante	AuthorityKeyIdentifier 2.5.29.35	Contiene un hash de 20 bytes del atributo clave pública del DIGILOGIX AC que emitió el certificado.
Uso Extendido de Clave	Extended Key Usage 2.5.29.37	Autenticación del cliente (1.3.6.1.5.5.7.3.2) Correo seguro (1.3.6.1.5.5.7.3.4) 2.5.29.37
SubjectAlternativeName (Nombres Alternativos del Suscriptor)	commonName 2.5.4.3	Nombres y Apellidos
	serialNumber 2.5.4.5	CUIT o CUIL y número del mismo
	title 2.5.4.12	Cargo o título del suscriptor dentro de la organización, debe corresponder con la certificación aportada en el proceso de autenticación

Acceso Información Emisor	AuthorityInfoAccess 1.3.6.1.5.5.7.1.1	[1] Authority Info Access Access Method=On-line Certificate Status Protocol (1.3.6.1.5.5.7.48.1) Alternative Name: URL=http://ocsp.digilogix.com.ar/ocsp [2] Authority Info Access Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2) Alternative Name: URL=http://www.digilogix.com.ar/ar/07.crt
Declaraciones de certificados calificados	QCStatement 1.3.6.1.5.5.7.1.3	OID=2.16.32.1.10.1, cuando las claves sean generadas por software. OID=2.16.32.1.10.2.1, cuando las claves sean generadas en dispositivos que cuenten con certificación FIPS 140 (Versión 2) nivel 1. OID=2.16.32.1.10.2.2, cuando las claves sean generadas en dispositivos que cuenten con certificación FIPS 140 (Versión 2) nivel 2. OID=2.16.32.1.10.2.3, cuando las claves sean generadas en dispositivos que cuenten con certificación FIPS 140 (Versión 2) nivel 3

c) Perfil del certificado de proveedores de otros servicios en relación con la FirmaDigital

Perfil del certificado de aplicaciones

Certificado x.509 v3 Atributos Extensiones	Valor/OID	Contenido
Versión	Version	2 Corresponde a versión 3
Número de serie	SerialNumber 2.5.4.5	Entero positivo asignado unívocamente por la AC DIGILOGIX a cada certificado
Algoritmo de Firma	signatureAlgoritm 2.5.8.3	sha256RSA 1.2.840.113549.1.1.11
	commonName 2.5.4.3	AC-DIGILOGIX

Issuer (Nombre distintivo del emisor)	serialNumber 2.5.4.5	CUIT 30714128716
	organizationName 2.5.4.10	DIGILOGIX S.A.
	stateOrProvinceName 2.5.4.8	Ciudad Autónoma de Buenos Aires
	countryName 2.5.4.6	AR
Validez (desde, hasta)	notBefore	(Válido desde) <fecha, hora, minutos ysegundos de emisión> Fecha y hora en que el período de vigencia del certificado comienza
	notAfter	(Válido hasta) <fecha,hora, minutos y segundos de emisión + 2años> Fecha y hora en que el periodo de vigencia del certificado termina
Subject DN (Nombre distintivo del suscriptor)	commonName 2.5.4.3	CN=Denominación de la Aplicación
	organizationName 2.5.4.10	O=Nombre de la Persona Jurídica Pública o Privada responsable de la aplicación
	organizationalUnitName 2.5.4.11	OU=Unidad Operativa relacionada con laaplicación
	serialNumber 2.5.4.5	serialNumber=CUIT y su número
	countryName 2.5.4.6	C=AR
SubjectPublicKeyInfo (Clave pública del suscriptor)	publickeyalgorithm	RSA 1.2.840.113549.1.1.1
	Publickeylength	2048 bits Longitud de la clave pública del suscriptor
	Public key	<Clave pública delsuscriptor> Valor de la clave pública del suscriptor
Extensiones del certificado (Extensions)		
Restricciones básicas	Basic Constraints 2.5.29.19	Tipo de asunto = Entidad final pathLenghtConstraint = Null

Usos de clave	Key Usage 2.5.29.15	digitalSignature = 1 contentCommitment = 1 keyEncipherment = 1 dataEncipherment = 1 keyAgreement = 0 keyCertSign = 0 cRLSign = 0 encipherOnly = 0 decipherOnly = 0
Identificador de clave del Suscriptor	Subject Key Identifier 2.5.29.14	Contiene un hash de 20 bytes del atributo clave pública del suscriptor
Puntos de Distribución de la Lista de Certificados Revocados	CRLDistributionPoints 2.5.29.31	[1] Punto de distribución CRL Dirección URL=http://www.digilogix.com.ar/ar/digilogix.crl [2] Punto de distribución CRL Dirección URL=http://backup.digilogix.com.ar/ar/digilogix.crl
Política de Certificación	CertificatePolicies 2.5.29.32	OID de la Política de Certificación de DIGILOGIX S.A OID=2.16.32.1.1.7 URL de la Política: https://www.digilogix.com.ar/documentos/cps.pdf Texto de aviso=certificado emitido por un certificador licenciado en el marcode la Ley 25.506
Identificador de la Clave de la Autoridad Certificante	AuthorityKeyIdentifier 2.5.29.35	Contiene un hash de 20 bytes del atributo clave pública del DIGILOGIX AC que emitió el certificado.
Uso Extendido de Clave	Extended Key Usage 2.5.29.37	Autenticación del cliente (1.3.6.1.5.5.7.3.2)
Acceso Información emisor	AuthorityInfoAccess 1.3.6.1.5.5.7.1.1	[1]Authority Info Access Access Method=On-line Certificate Status Protocol (1.3.6.1.5.5.7.48.1) Alternative Name: URL=http://ocsp.digilogix.com.ar/ocsp [2]Authority Info Access Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2) Alternative Name: URL=http://www.digilogix.com.ar/ar/07.crt

Declaraciones de certificados calificados	QCStatement 1.3.6.1.5.5.7.1.3	OID=2.16.32.1.10.1, cuando las claves sean generadas por software. OID=2.16.32.1.10.2.1, cuando las claves sean generadas en dispositivos que cuenten con certificación FIPS 140 (Versión 2) nivel 1. OID=2.16.32.1.10.2.2, cuando las claves sean generadas en dispositivos que cuenten con certificación FIPS 140 (Versión 2) nivel 2. OID=2.16.32.1.10.2.3, cuando las claves sean generadas en dispositivos que cuenten con certificación FIPS 140 (Versión 2) nivel 3.

Perfil del certificado de Autoridad de Sello de Tiempo

Campos Atributos Extensiones	Nombre del campo y OID	Contenido
Versión	Version	2 Corresponde a versión 3
Número de serie	SerialNumber 2.5.4.5	Entero positivo asignadounívocamente por la AC DIGILOGIX a cada certificado
Algoritmo de Firma	signatureAlgoritm	sha256RSA 1.2.840.113549.1.1.11
Issuer (Nombre distintivo del emisor)	commonName 2.5.4.3	AC-DIGILOGIX
	serialNumber 2.5.4.5	30714128716
	organizationName 2.5.4.10	DIGILOGIX S.A.
	stateOrProvinceName 2.5.4.8	Ciudad Autónoma de Buenos Aires
	countryName 2.5.4.6	AR
Validez (desde, hasta)	notBefore	(Válido desde) <fecha, hora, minutos ysegundos de emisión> Fecha y hora en que el período de vigencia del certificado comienza
	notAfter	(Válido hasta) <fecha,hora, minutos y segundos de emisión + 2años>

		Fecha y hora en que el periodo de vigencia del certificado termina
Subject DN (Nombre distintivo del suscriptor)	commonName 2.5.4.3	CN=Denominación del servicio de emisiónde sello de tiempo
	organizationName 2.5.4.10	O=Unidad Operativa relacionada con el suscriptor
	organizationalUnitName 2.5.4.11	OU=Nombre de la Persona Jurídica Públicao Privada responsable del servicio
	serialNumber 2.5.4.5	serialNumber=CUIT y su número
	countryName 2.5.4.6	C=AR
SubjectPublicKeyInfo	publickeyalgorithm	RSA 1.2.840.113549.1.1.1
	Publickeylength	2048 bits Longitud de la clave pública
	Public key	<Clave pública delsuscriptor> Valor de la clave pública
Extensions (Extensiones del certificado)		
Restricciones básicas	Basic Constraints 2.5.29.19	Tipo de asunto = Entidad final pathLenghtConstraint = Null
Usos de clave	Key Usage 2.5.29.15	digitalSignature = 1 contentCommitment = 1 keyEncipherment =1 dataEncipherment = 1 keyAgreement = 0 keyCertSign = 0 cRLSign = 0 encipherOnly = 0 decipherOnly = 0
Identificador de clave del Suscriptor	Subject Key Identifier 2.5.29.14	Contiene un hash de 20 bytes del atributo clave pública del suscriptor
Puntos de Distribución de la Lista de Certificados Revocados	CRLDistributionPoints 2.5.29.31	Punto de distribución CRL Dirección URL=http://www.digilogix.com.ar/ar/digilogix.crl Punto de distribución CRL Dirección URL=http://backup.digilogix.com.ar/ar/digilogix.crl

Política de Certificación	CertificatePolicies 2.5.29.32	OID de la Política de Certificación de DIGILOGIX S.A OID=2.16.32.1.1.7 URL de la Política: https://www.digilogix.com.ar/documentos/cps.pdf Texto de aviso=certificado emitido por un certificador licenciado en el marco de la Ley 25.506
Identificador de la Clave de la Autoridad Certificante	AuthorityKeyIdentifier 2.5.29.35	Contiene un hash de 20 bytes del atributo clave pública del DIGILOGIX AC que emitió el certificado.
Uso Extendido deClave	Extended Key Usage 2.5.29.37	Autenticación del cliente (1.3.6.1.5.5.7.3.2) Certificación digital de fecha y hora (1.3.6.1.5.5.7.3.8)
Acceso Información emisor	AuthorityInfoAccess 1.3.6.1.5.5.7.1.1	[1]Authority Info Access Access Method=On-line Certificate Status Protocol (1.3.6.1.5.5.7.48.1) Alternative Name: URL=http://ocsp.digilogix.com.ar/ocsp [2]Authority Info Access Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2) Alternative Name: URL=http://www.digilogix.com.ar/ar/07.crt
Declaraciones de certificados calificados	QCStatement 1.3.6.1.5.5.7.1.3	OID=2.16.32.1.10.2.3, clave generada en dispositivos que cuenten con certificación FIPS 140 (Versión 2) nivel 3.

Perfil del certificado de Autoridad de Sello de Competencia

Certificado x.509 v3 Atributos Extensiones	Nombre del campo y OID	Contenido
Versión	Version	2 Corresponde a versión 3
Número de serie	SerialNumber 2.5.4.5	Entero positivo asignado unívocamente por la AC DIGILOGIX a cada certificado
Algoritmo de Firma	signatureAlgoritm	sha256RSA 1.2.840.113549.1.1.11
Issuer (Nombre	commonName 2.5.4.3	AC-DIGILOGIX
	serialNumber 2.5.4.5	30714128716
	organizationName	DIGILOGIX S.A.

distintivo del emisor)	2.5.4.10	
	stateOrProvinceName 2.5.4.8	Ciudad Autónoma de Buenos Aires
	countryName 2.5.4.6	AR
Validez (desde, hasta)	notBefore	(Válido desde) <fecha, hora, minutos ysegundos de emisión> Fecha y hora en que el período de vigencia del certificado comienza
	notAfter	(Válido hasta) <fecha,hora, minutos y segundos de emisión + 2años> Fecha y hora en que el periodo de vigencia del certificado termina
Subject DN (Nombre distintivo del suscriptor)	commonName 2.5.4.3	Denominación del servicio de emisión de sello de competencia
	organizationName 2.5.4.10	Nombre de la Persona Jurídica Pública o Privada responsable de la aplicación
	organizationalUnitName 2.5.4.11	Unidad Operativa relacionada con la aplicación
	serialNumber 2.5.4.5	CUIT y su número
	countryName 2.5.4.6	AR
SubjectPublicKeyInfo (Clave pública del suscriptor)	publickeyalgorithm	RSA 1.2.840.113549.1.1.1
	Publickeylength	2048 bits Longitud de la clave pública del suscriptor
	Public key	<Clave pública delsuscriptor> Valor de la clave pública del suscriptor
Extensions (Extensiones del certificado)		
Basic Constraints (Restricciones básicas)	2.5.29.19	Tipo de asunto = Entidad final pathLenghtConstraint = Null
Key Usage (Usos de clave)	2.5.29.15	digitalSignature = 1 contentCommitment = 1 keyEncipherment = 1 dataEncipherment = 0 keyAgreement = 0 keyCertSign = 0 cRLSign = 0 encipherOnly = 0 decipherOnly = 0

Subject Key Identifier (Identificador de clave del Suscriptor)	2.5.29.14	Contiene un hash de 20 bytes del atributo clave pública del suscriptor
Puntos de Distribución de la Lista de Certificados Revocados	CRLDistributionPoints 2.5.29.31	[3] Punto de distribución CRL Dirección URL=http://www.digilogix.com.ar/ar/digilogix.crl [4] Punto de distribución CRL Dirección URL=http://backup.digilogix.com.ar/ar/digilogix.crl
Política de Certificación	CertificatePolicies 2.5.29.32	OID de la Política de Certificación de DIGILOGIX S.A OID=2.16.32.1.1.7 URL de la Política: https://www.digilogix.com.ar/document os/cps.pdf Texto de aviso=certificado emitido por un certificador licenciado en el marco de la Ley 25.506
Identificador de la Clave de la Autoridad Certificante	AuthorityKeyIdentifier 2.5.29.35	Contiene un hash de 20 bytes del atributo clave pública del DIGILOGIX AC que emitió el certificado.
Uso Extendido deClave	Extended Key Usage 2.5.29.37	Autenticación del cliente (1.3.6.1.5.5.7.3.2)
Acceso Información emisor	AuthorityInfoAccess 1.3.6.1.5.5.7.1.1	[1]Authority Info Access Access Method=On-line CertificateStatus Protocol (1.3.6.1.5.5.7.48.1) Alternative Name: URL=http://ocsp.digilogix.com.ar/ocsp[2]Authority Info Access Access Method=Certification AuthorityIssuer (1.3.6.1.5.5.7.48.2) Alternative Name: URL=http://www.digilogix.com.ar/ar/07.crt
Declaraciones de certificados calificados	QCStatement 1.3.6.1.5.5.7.1.3	OID=2.16.32.1.10.2.3, clave generada en dispositivos que cuenten con certificación FIPS 140 (Versión 2) nivel 3

7.2.- Perfil de la Lista de Certificados Revocados

Campos Atributos Extensiones	Valor/OID	Observaciones
Versión	Version	1 Corresponde a versión 2
Algoritmo de Firma	signatureAlgoritm	sha256RSA 1.2.840.113549.1.1.11
Issuer (Nombre distintivo del emisor)	commonName 2.5.4.3	AC-DIGILOGIX
	serialNumber 2.5.4.5	CUIT 30714128716
	organizationName 2.5.4.10	DIGILOGIX S.A.
	stateOrProvinceName 2.5.4.8	Ciudad Autónoma de Buenos Aires
	countryName 2.5.4.6	AR
Validity (Not before, not after) Validez (desde, hasta)		
Día y hora de vigencia	thisUpdate	<fecha y hora UTC> yyyy/mm/ddhh:mm:sshuso-horario Fecha y hora efectivas de emisión, a partir de la cual entre en vigencia
Próxima Actualización	nextUpdate	<fecha y hora UTC> yyyy/mm/ddhh:mm:ss huso-horario Fecha y hora de emisión de la próxima Lista de Certificados Revocados
Identificador de la Clave de la Autoridad Certificante	AuthorityKeyIdentifier 2.5.29.35	Contiene un hash de 20 bytes del atributo clave pública del DIGILOGIX AC que emitió la Lista de Certificados Revocados.
Número de CRL	CRL Number 2.5.29.20	Número incremental que identifica la CRL emitida
CRL más reciente	freshestCRL 2.5.29.46	Ubicación de la CRL más reciente

Indicador Delta CRL	Delta CRL Indicator 2.5.29.27	Número que se incrementa cada vez que se emite una Delta CRL
Certificados Revocados (RevokedCertificates)		
Fecha de Revocación	<fecha y hora UTC> yyyy/mm/ddhh:mm:ss huso-horario	Fecha y hora en que se revocó el certificado
Número de Serie del Certificado revocado	Serial Number hasta 20 octetos 2.5.4.5	Número de Serie del Certificado revocado
Motivo de la Revocación	ReasonCode 2.5.29.21	Motivo de la Revocación
Versión de CA	V0.0	Versión de CA

7.3.- Perfil del Certificado del Servicio de Consulta OCSP

Campos Atributos Extensiones	Valor/OID	Contenido
Versión	Version	2 Corresponde a versión 3
Número de serie	SerialNumber 2.5.4.5	Entero positivo asignado unívocamente por la AC DIGILOGIX a cada certificado
Algoritmo de Firma	signatureAlgoritm	sha256RSA 1.2.840.113549.1.1.11
Issuer (Nombre distintivo del emisor)		
Issuer (Nombre distintivo del emisor)	commonName 2.5.4.3	AC-DIGILOGIX
	serialNumber 2.5.4.5	CUIT 30714128716
	organizationName 2.5.4.10	DIGILOGIX S.A.
	stateOrProvinceName 2.5.4.8	Ciudad Autónoma de Buenos Aires
	countryName 2.5.4.6	AR
Validez (desde, hasta)	notBefore	<fecha, hora, minutos ysegundos de emisión> Fecha y hora en que el período de vigencia del certificado comienza
	notAfter	<fecha,hora, minutos y segundos de emisión + 2años> Fecha y hora en que el periodo de vigencia del certificado termina

Nombre distintivo del suscriptor (Subject)	commonName 2.5.4.3	AC-DIGILOGIX
	serialNumber 2.5.4.5	CUIT 30714128716
	organizationName 2.5.4.10	DIGILOGIX S.A.
	stateOrProvinceName 2.5.4.8	Ciudad Autónoma de Buenos Aires
	countryName 2.5.4.6	AR
SubjectPublicKeyInfo (Clave pública del suscriptor)	publickeyalgorithm	Tipo de algoritmo de clave pública utilizado
	Publickeylength	Longitud de la clave pública del suscriptor
	Public key	Valor de la clave pública del suscriptor
Extensions (Extensiones del certificado)		
Restricciones básicas	Basic Constraints 2.5.29.19	Tipo de asunto = Entidad final pathLenghtConstraint = Null
Usos de clave	Key Usage 2.5.29.15	digitalSignature = 1 contentCommitment= 1 keyEncipherment = 0 dataEncipherment = 0 keyAgreement = 0 keyCertSign = 0 cRLSign = 0 encipherOnly = 0 decipherOnly = 0
Identificador de clave del Suscriptor	Subject Key Identifier 2.5.29.14	Contiene un hash de 20 bytes del atributo clave pública del suscriptor
Puntos de Distribución de la Lista de Certificados Revocados	CRLDistributionPoints 2.5.29.31	Punto de distribución CRL Dirección URL=http://www.digilogix.com.ar/ar/digilogix.crl Punto de distribución CRL Dirección URL=http://backup.digilogix.com.ar/ar/digilogix.crl

Política de Certificación	CertificatePolicies 2.5.29.32	OID de la Política de Certificación de DIGILOGIX S.A OID=2.16.32.1.1.7 URL de la Política: https://www.digilogix.com.ar/documen t os/cps.pdf Texto de aviso=certificado emitido por un certificador licenciado en el marco de la Ley 25.506
Identificador de la Clave de la Autoridad Certificante	AuthorityKeyIdentifier 2.5.29.35	Contiene un hash de 20 bytes del atributo clave pública del DIGILOGIX AC que emitió el certificado.
Uso Extendido deClave	Extended Key Usage 2.5.29.37	OCSPSigning (1.3.6.1.5.5.7.3.9) Corresponde a las respuestas del servicio OCSP
Acceso Información emisor	AuthorityInfoAccess 1.3.6.1.5.5.7.1.1	[1]Authority Info Access Access Method=On-line Certificate Status Protocol (1.3.6.1.5.5.7.48.1) Alternative Name: URL=http://ocsp.digilogix.com.ar/ocsp [2]Authority Info Access Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2) Alternative Name: URL=http://www.digilogix.com.ar/ar/07 .crt

8.- AUDITORIA DE CUMPLIMIENTO Y OTRAS EVALUACIONES

DIGILOGIX S.A., en su carácter de Certificador Licenciado, se encuentra sujeto a las auditorías dispuestas en el art. 34 de la Ley N° 25.506 y su modificatoria.

Asimismo, se encuentra sujeta a inspecciones extraordinarias realizadas u ordenadas por la SECRETARÍA DE INNOVACIÓN PÚBLICA, en cumplimiento con la Resolución N° 946/21.

Las auditorías se realizan en base a los programas de trabajo que son generados por la Autoridad de Aplicación, los que son comunicados e informados oportunamente.

Los aspectos a evaluar se encuentran establecidos en el art. 27 de la Ley N° 25.506 y otras normas reglamentarias.

Los informes resultantes de las auditorías son elevados a la SECRETARÍA DE INNOVACIÓN PÚBLICA.

Sus aspectos relevantes son publicados en forma permanente e ininterrumpida en el sitio web de AC - DIGILOGIX: https://www.digilogix.com.ar/documentos

Por su parte, AC - DIGILOGIX, en su carácter de Certificador Licenciado, realizará auditorías periódicas a sus propias Autoridades de Registro autorizadas a funcionar, con el objeto de verificar el cumplimiento de los procesos y procedimientos establecidos en la normativa regulatoria de Firma Digital.

El certificador cumple las exigencias reglamentarias impuestas por:

a) Los artículos 33 y 34 de la Ley Nº 25.506 de Firma Digital, respecto al sistema de auditoría y el artículo 21, inciso k) de la misma ley, relativo a la publicación de informes de auditoría.

b) Los art. 6, 7 y 8 del Decreto Nº 182/19, relativos al sistema de auditoría.

9. – ASPECTOS LEGALES Y ADMINISTRATIVOS

9.1. – Aranceles

Los certificados digitales emitidos bajo la Política y el presente Manual son expedidos a favor de Personas Humanas y/o Jurídicas a título oneroso, aplicándose aranceles diferenciales asociados a los distintos tipos de certificados.

9.2. - Responsabilidad Financiera

Las responsabilidades financieras se originan en lo establecido por la Ley N° 25.506 y su Decreto Reglamentario Nº 182/19 y en las disposiciones del presente Manual.

9.3. – Confidencialidad

Se especifica la información a ser tratada como confidencial por **AC - DIGILOGIX** y por las Autoridades de Registro operativamente vinculadas, de acuerdo con lo establecido por las normas legales y reglamentarias vigentes.

9.3.1. - Información confidencial

Toda información remitida por el solicitante o suscriptor de un certificado al momento de efectuar un requerimiento es considerada confidencial y no es divulgada a terceros sin su consentimiento previo y expreso, salvo que sea requerida mediante resolución fundada en causa judicial por juez competente. 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.

Digilogix SA, 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 y el presente Manual. 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 **AC - DIGILOGIX**.
- 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 Continuidad de operaciones, controles, procedimientos de seguridad y registros de auditoría pertenecientes al Certificador.

En todos los casos resulta de aplicación la Ley N° 25.326 de protección de datos personales, su reglamentación y normas complementarias.

9.3.2. - Información no confidencial

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

a) Contenido de los certificados y de las listas de certificados revocados.

b) Información sobre Personas Humanas o Jurídicas que se encuentre disponible en certificados o en directorios de acceso público.

c) Políticas de Certificación y Manual de Procedimientos de Certificación (en sus aspectos no confidenciales).

d) Secciones públicas de la Política de Seguridad de **AC - DIGILOGIX**

e) Política de privacidad de **AC - DIGILOGIX**

9.3.3. – Responsabilidades de los roles involucrados

La información confidencial podrá ser revelada ante un requerimiento emanado de juez competente como parte de un proceso judicial o ante requerimiento de autoridad administrativa como parte de un proceso administrativo.
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 sólo podrá efectuarse previa autorización escrita del suscriptor del certificado.
No será necesario el consentimiento cuando:

- Los datos se hayan obtenido de fuentes de acceso público irrestricto;
- Los datos se limiten a nombre, Documento Nacional de Identidad, identificación tributaria o previsional u ocupación.
- Aquellos para los que **AC - DIGILOGIX** hubiera obtenido autorización expresa de su titular.

9.4. – Privacidad

Todos los aspectos vinculados a la privacidad de los datos personales se encuentran sujetos a la normativa vigente en materia de Protección de los Datos Personales (Ley Nº 25.326 y normas reglamentarias, complementarias y aclaratorias). Las consideraciones particulares se incluyen en la Política de Privacidad.

9.5 - Derechos de Propiedad Intelectual

El derecho de autor de los sistemas y aplicaciones informáticas desarrollados por el Certificador para la implementación de su AC, como así toda la documentación relacionada, pertenece a **DIGILOGIX S.A.**
Consecuentemente, dichos documentos no pueden ser reproducidos, copiados ni utilizados de ninguna manera, total o parcial, sin previo y formal consentimiento de **DIGILOGIX S.A.**, de acuerdo a la legislación vigente.

9.6. – Responsabilidades y garantías

Las responsabilidades y garantías para **AC - DIGILOGIX**, sus Autoridades de Registro, los suscriptores, los terceros usuarios y otras entidades participantes, se rigen por lo establecido por la Ley N° 25.506, su Decreto Reglamentario Nº 182/19, la Resolución N° 946/21 y toda otra normativa complementaria.
Asimismo, las partes contratantes se rigen por el Acuerdo con Suscriptores, como contrato específico que regula la relación entre el suscriptor y el Certificador Licenciado **DIGILOGIX S.A.**

9.7. – Deslinde de responsabilidad

Las limitaciones de responsabilidad del Certificador Licenciado se rigen por lo establecido en el art. 39 de la Ley N° 25.506, en las disposiciones del presente Manual y en el Acuerdo con Suscriptores.

9.8. – Limitaciones a la responsabilidad frente a terceros

Las limitaciones de responsabilidad del certificador licenciado respecto a otras entidades participantes, se rigen por lo establecido en el art. 39 de la Ley N° 25.506, en las disposiciones del presente Manual y en los Términos y Condiciones con terceros usuarios.

9.9. – Compensaciones por daños y perjuicios

No aplicable.

9.10. – Condiciones de vigencia

El presente Manual se encuentra vigente con su aprobación por parte del Ente Licenciante, a partir de la fecha en la cual el correspondiente acto administrativo sea publicado en el Boletín Oficial de la República Argentina. La misma tendrá vigencia hasta tanto sea reemplazada por una nueva versión.

Todo cambio en el Manual, una vez aprobado por el Ente Licenciante, será debidamente comunicado al suscriptor.

9.11.- Avisos personales y comunicaciones con los participantes

No aplicable.

9.12.- Gestión del ciclo de vida del documento

9.12.1. - Procedimientos de cambio

En caso de ser necesario efectuar modificaciones a este Manual de Procedimientos, las mismas serán remitidas al Ente Licenciante para su aprobación. En caso de ser requerido, se informará al Ente Licenciante las causas que motivaron la necesidad de la modificación.

Una vez notificada la aprobación de las modificaciones al Manual de Procedimientos por parte del Ente Licenciante, la **AC - DIGILOGIX S.A.** publicará en su sitio web la nueva versión del documento.

Copias del Manual de Procedimientos vigente y de sus versiones anteriores se encuentran disponibles en la interfaz web de la **AC – DIGILOGIX** en: http://www.digilogix.com.ar/documentos

El Manual de Procedimientos emitido por la **AC – DIGILOGIX**, así como cualquier modificación a efectuar al mismo o cualquier cambio en los datos relativos a su licencia, serán sometidos a aprobación por parte del Ente Licenciante.

Esto también es aplicable a la Política Única de Certificación de DIGILOGIX S.A.

9.12.2 – Mecanismo y plazo de publicación y notificación

Una copia de la versión vigente del Manual de Procedimientos se encuentra disponible en forma pública y accesible a través de Internet en el sitio web http://www.digilogix.com.ar/documentos como así también del resto de los documentos.

9.12.3. – Condiciones de modificación del OID

No aplicable.

9.13. - Procedimientos de resolución de conflictos

Cualquier controversia y/o conflicto resultante de la aplicación de este Manual de Procedimientos, deberá ser resuelto en sede administrativa de acuerdo a las previsiones de la Ley Nacional de Procedimientos Administrativos N° 19.549 y su Decreto Reglamentario N° 894/17.

El presente Manual se encuentra en un todo subordinada a las prescripciones de la Ley N° 25.506 y su reglamentación.

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 DIGILOGIX SA, en su condición de Certificador Licenciado.

Una vez recibido el reclamo en las oficinas de DIGILOGIX SA 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. Dará traslado del acta, mediante notificación fehaciente, a las partes involucradas, Autoridad de Registro y/o Suscriptor y/o Tercero Usuario. Estas partes dispondrán un plazo de DIEZ (10) días corridos para ofrecer y producir prueba que haga a su defensa y aleguen sobre el mérito de la misma.

Finalmente, DIGILOGIX SA resolverá en un plazo de diez (10) días corridos conforme a los criterios de máxima razonabilidad, equidad y pleno ajuste al bloque de legalidad vigente y aplicable.

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 a la vía judicial correspondiente.

En ningún caso el Manual de Procedimientos del certificador prevalecerá sobre lo dispuesto por la normativa legal vigente de Firma Digital.

9.14. - Legislación aplicable

La legislación que respalda la interpretación, aplicación y validez de este Manual de Procedimientos es la Ley Nº 25.506, el Decreto Nº 182/19, la Resolución N° 946/21 y toda otra norma complementaria dictada por la autoridad competente.

9.15. – Conformidad con normas aplicables

La legislación aplicable a la actividad del Certificador es la Ley Nº 25.506, el Decreto Nº 182/19, toda otra norma complementaria dictada por la autoridad competente y otras normas que sean aplicables.

9.16. – Cláusulas adicionales

No se establecen cláusulas adicionales.

9.17. – Otras cuestiones generales

Versión y Modificación	Fecha de emisión	Revisado por	Descripción

Versión 1.0	22/05/2015	Directorio DIGILOGIX	Aprobación para presentación
Versión 2.0	Desde la publicación en B.O.	Directorio DIGILOGIX	Renovación de licencia

República Argentina - Poder Ejecutivo Nacional
Las Malvinas son argentinas

Hoja Adicional de Firmas
Anexo

Número: IF-2022-91402878-APN-SSIA#JGM

CIUDAD DE BUENOS AIRES
Miércoles 31 de Agosto de 2022

Referencia: Manual de Procedimientos - DIGILOGIX SA

El documento fue importado por el sistema GEDO con un total de 63 pagina/s.

Digitally signed by Gestion Documental Electronica
Date: 2022.08.31 11:20:06 -03:00

Luis Mariano PAPAGNI
Subsecretario
Subsecretaría de Innovación Administrativa
Jefatura de Gabinete de Ministros

Digitally signed by Gestion Documental Electronica
Date: 2022.08.31 11:20:07 -03:00