MANUAL DE PROCEDIMIENTOS

POLÍTICA ÚNICA DE CERTIFICACIÓN DE DIGILOGIX S.A.

CERTIFICADOR LICENCIADO

DIGILOGIX S.A.

Versión 4.0

Febrero 2025

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, los Decretos Nos. 182/19 y 743/24, la Resolución de la Secretaría de Innovación, Ciencia y Tecnología dependiente de la Jefatura de Gabinete de Ministros N° 11/2025 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: 4.0
   Lugar o sitio de publicación: se publica en el sitio web de la **AC-DIGILOGIX** (https://www.digilogix.com.ar/documentos/)
d) Fecha de aplicación: A partir de su aprobación por el Ente Licenciante
e) 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 presentan una solicitud de emisión, dado el tipo de información que manejan y su cercanía al usuario final. Tal como indica la Resolución SICYT N° 11/2025, **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 se incorporará en la lista correspondiente en el sitio web de **DIGILOGIX S.A.** con los datos completos de contacto, es decir, nombre, dirección y teléfono. Lista de Autoridades de Registro: https://www.digilogix.com.ar/

1.3.3.- Suscriptores 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 SICYT N° 11/2025, Anexo I Capítulo V Artículo 33.
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.

1.3.4.- Terceros usuarios

Son Terceros Usuarios de los certificados emitidos bajo la Política Única de Certificación asociada a este manual, 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 Política Única de Certificación asociada a este manual 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 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

El presente Manual de Procedimientos se presenta ante la SUBSECRETARÍA DE INNOVACIÓN dependiente de la SECRETARÍA DE INNOVACIÓN, CIENCIA Y TECNOLOGÍA de la JEFATURA DE GABINETE DE MINISTROS.

1.6. - Definiciones y Acrónimos

1.6.1. - Definiciones

- Autoridad de Aplicación: la SECRETARÍA DE INNOVACIÓN, CIENCIA Y TECNOLOGÍA dependiente de la JEFATURA DE GABINETE DE MINISTROS es la Autoridad de Aplicación de firma digital en la REPÚBLICA ARGENTINA.
- Autoridad de Registro: es la entidad que tiene a su cargo las funciones de:
    - 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 DIGILOGIX S.A. con el que se encuentre vinculada, en la parte que resulte aplicable.
- Cumplimiento de las Pautas Técnicas y de Procedimientos para la Toma de Datos Biométricos dispuestas en la Resolución SICYT N° 11/2025, que establecen los requisitos para la captura de la fotografía digital del rostro y la huella dactilar de los solicitantes y suscriptores de firma digital.
- Cumplimiento con el Decreto N° 743/24 y su reglamentación, Resolución SICYT N° 11/2025, en los casos de presencia telemática del suscriptor/solicitante
- Habilitación de Contingencia por fallos del RENAPER: Cumplimiento de la validación de identidad con presencia física habilitando como contingencia la posibilidad de finalizar el trámite ante fallos relacionados con el servicio que presta el RENAPER; haciendo la validación de la identidad con el número ID del Documento Nacional de Identidad a través del sistema proporcionado por el mencionado Registro Nacional de las Personas.
- Cumplimiento de la conservación y guarda de toda la documentación y antecedentes vinculados a la habilitación de la contingencia.

Dichas funciones son delegadas por la AC DIGILOGIX en las Autoridades de Registro. Pueden 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).
- Autoridad de Sello de Tiempo: Entidad que acredita la fecha y hora cierta, asignada a un documento o registro electrónico por una tercera parte confiable y firmada digitalmente por ella.
- Autoridad de Sello de Competencia: Entidad que acredita competencias, roles, funciones o relaciones laborales del titular de un certificado de firma digital.
- Ente Licenciante: La SECRETARÍA DE INNOVACIÓN, CIENCIA Y TECNOLOGÍA de la JEFATURA DE GABINETE DE MINISTROS juntamente con la SUBSECRETARÍA DE INNOVACIÓN constituyen el Ente Licenciante.
- 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).
- Certificados de Aplicación: Definidos como aquellos que tienen la finalidad de identificar a la aplicación o servicio que firma documentos digitales o registros en forma automática mediante un sistema informático programado a tal fin.
- Infraestructura tecnológica del Certificador Licenciado: Conjunto de servidores y otros equipamientos informáticos relacionados, software y dispositivos criptográficos utilizados para la generación, almacenamiento y publicación de los certificados digitales emitidos por el certificador licenciado, para la provisión de información sobre su estado de validez y para la prestación de otros servicios en relación a la firma digital enumerados en la Resolución SICYT N° 11/2025 Anexo I Capítulo V Artículo 33. La infraestructura tecnológica que soporta los servicios del certificador utilizada tanto en el establecimiento principal como en el alternativo destinado a garantizar la continuidad de sus operaciones, deberá estar situada en territorio argentino, bajo el control del certificador licenciado y afectada a tareas específicas propias de certificación, de custodia centralizada de claves privadas y demás servicios asociados a firma digital.
- 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 Contingencia: 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 Certificados Revocados (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
ARCA - Agencia de Recaudación y Control Aduanero
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
RENAPER – Registro Nacional de las Personas
RFC - RequestforComments
RSA - Rivest, Shamir y Adleman
SHA - Secure Hash Algorithm
SICYT – SECRETARÍA DE INNOVACIÓN, CIENCIA Y TECNOLOGÍA
SSI – SUBSECRETARÍA DE INNOVACIÓN
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:

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

ingresando el número de serie del certificado digital del que se quiera obtener 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 parties*")
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://suscriptor.digilogix.com.ar/CertificadoSuscriptor/EstadosCertificados
j) Listado de AR. Se puede consultar en: https://www.digilogix.com.ar
k) La lista de Certificados Revocados (CRL) en:
   http://www.digilogix.com.ar/ar/digilogixv3.crl
   http://backup.digilogix.com.ar/ar/digilogixv3.crl
   http://www.digilogix.com.ar/ar/digilogixv3+.crl
   http://backup.digilogix.com.ar/ar/digilogixv3+.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**.

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 la 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

En esta sección se describen los procedimientos empleados para autenticar la identidad de los solicitantes de certificados digitales y utilizados por AC-DIGILOGIX o sus Autoridades de Registro como prerrequisito para su emisión. También se describen los pasos para la autenticación de los solicitantes de renovación y revocación de certificados.

3.1.- Asignación de nombres de suscriptores

3.1.1.- Tipos de Nombres

El nombre a utilizar es el que surge de la documentación presentada por el solicitante, de acuerdo al apartado que sigue.

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]"

El valor posible para el campo [tipo de documento] es "CUIT" o "CUIL": Clave Única de Identificación Tributaria o Laboral (según corresponda). En el caso que el suscriptor sea extranjero deberá contar

con DNI y CUIL argentino.• “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: IF-2025-95380015-APN-SSI#JGM

• “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 Artículo 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. El almacenamiento y la utilización de las claves se realizarán bajo el estricto control del suscriptor, garantizando la confidencialidad e integridad de las mismas. Este procedimiento cumple con lo establecido en el inciso b) del Artículo 21 de la Ley N° 25.506 y en la Resolución SICYT N° 11/2025, que regula la emisión de certificados digitales con almacenamiento de claves en custodia.

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 representante a quien se le tome la fotografía del rostro y la huella dactilar a través de un dispositivo biométrico en caso de ser presencial. En caso de que sea Telemática será en concordancia con las Pautas Técnicas y de Procedimientos para la Toma de Datos Biométricos establecidas en la Resolución SICYT N° 11/2025. Utilizando los servicios de RENAPER en ambos casos.

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.

d) De tratarse de Personas Jurídicas Privadas, registro con los documentos que se detallan más abajo con copias certificadas por Escribano Público de corresponder:
e) Estatuto o Contrato Social correspondiente a la Persona Jurídica o documento análogo.
f) Documento que acredite la personería legal, acta de distribución de cargos o documento equivalente, según el tipo societario.
En el caso de apoderados generales, deberá presentarse un poder general amplio.
En todos los otros casos, se requerirá el acta de directorio o un poder especial que autorice la solicitud del certificado de firma digital.
g) Constancia de inscripción en el Registro Público de Comercio o documento análogo.
h) Constancia de inscripción en ARCA.
i) En caso de sociedades irregulares el DNI de todos los socios.
j) 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

Se describen los procedimientos de autenticación de la identidad de los suscriptores de los certificados de Personas Humanas.

La documentación a presentarse según sea el solicitante o suscriptor, será la siguiente:

- De poseer nacionalidad argentina, se requiere Documento Nacional de Identidad.
- De tratarse de extranjeros, se requiere Documento Nacional de Identidad argentino.

Se consideran obligatorias las exigencias reglamentarias impuestas por:

a) El Artículo 21, Inciso i) de la Ley Nº 25.506 relativo a la conservación de la documentación de respaldo de los certificados emitidos.
b) El Artículo 21, Inciso f) de la Ley Nº 25.506 relativo a la recolección de datos personales.
c) El Artículo 21, Capítulo II Inciso 3) del Decreto Nº 182/2019 relativo a generar, exigir o tomar conocimiento de la clave privada del suscriptor.
d) El Artículo 21, Inciso 14, Capítulo II del Decreto Nº 182/2019 relativo a la protección de datos personales.
Adicionalmente, **AC-DIGILOGIX** celebra UN (1) acuerdo con el solicitante o suscriptor, del que surge su conformidad respecto a la veracidad de la información incluida en el certificado.
En los casos de presencia física la Autoridad de Registro verifica que el dispositivo criptográfico utilizado por el solicitante, si fuera el caso, cumple con las especificaciones técnicas establecidas por el ente licenciante.

La **AC-DIGILOGIX** en los casos de emisión con presencia telemática actúa conforme a lo establecido en el Decreto N° 743/24. La validación de la identidad del suscriptor o del solicitante se realiza a través de los servicios de validación biométrica que presta el Registro Nacional de las Personas y conforme a las Pautas Técnicas y de Procedimientos para la Toma de Datos Biométricos dispuestas por la Resolución SICYT N° 11/2025, garantizando el mencionado Registro la validez y precisión del proceso de validación, y la custodia de manera segura las evidencias generadas.

e) En los casos de emisión con presencia física en concordancia con las Pautas Técnicas y de Procedimientos para la Toma de Datos Biométricos dispuestas por la Resolución SICYT N° 11/2025, AC – DIGILOGIX, y las Autoridades de Registro cumplen con la captura de fotografía digital del rostro y la huella dactilar a través de un dispositivo biométrico de los solicitantes de firma digital.

   El procedimiento de autenticación de la identidad de Personas Humanas, en todas sus modalidades (presencial y telemática), se encuentra detallado en el apartado 4.1.2 del presente Manual.

   DIGILOGIX S.A. garantiza en todos los casos el cumplimiento de los requisitos legales y técnicos previstos en la Ley N° 25.506, el Decreto N° 182/19, el Decreto N° 743/24 y la Resolución SICYT N° 11/2025.

3.2.4 – Protocolo de Contingencia ante Fallos en el Sistema de Biometría para la Validación de Identidad

Habilitación de contingencia: en los casos en que el solicitante y/o suscriptor adopte la modalidad presencia telemática para la solicitud, renovación o revocación de un certificado de firma digital, ante DOS (2) intentos fallidos del proceso de validación de la identidad de la plataforma del Registro Nacional de las Personas se habilitará para validar la identidad, en modalidad presencia física, con el número de trámite del DNI utilizando el servicio del Sistema de Identidad Digital (SID) que pone a disposición el mencionado Registro Nacional de las Personas.

3.2.5 - 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 Artículo 14 de la Ley N° 25.506.

3.2.6 - 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.

3.2.7- 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

En el caso de certificados digitales de Persona Humana o Jurídica, la renovación en este apartado aplica a la generación de UN (1) nuevo par de claves y su correspondiente certificado:

a) después de la revocación de UN (1) certificado

b) después de la expiración de UN (1) certificado

c) antes de la expiración de UN (1) certificado

En los casos a) y b) se exigirá el cumplimiento de los procedimientos previstos en el punto 3.2.3. - Autenticación de la identidad de Persona Humana y 3.2.2. Autenticación de la identidad de Personas Jurídicas Públicas o Privadas.

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

La generación de un certificado con el mismo par de claves no es admitida por la **AC- DIGILOGIX**.

3.4. - Requerimiento de revocación

a) Online con pin de revocación:
   - Ingresando al sitio web de la **AC-DIGILOGIX** a la siguiente URL: https:// suscriptor.digilogix.com.ar/ utilizando los datos de acceso, es decir, el email registrado y la contraseña que estableció en el inicio del trámite.
   - Buscar el certificado en el listado presentado y presionar REVOCAR
   - Establecer el motivo, ingresar el PIN de revocación y presionar nuevamente REVOCAR

b) Personalmente presentándose a la Autoridad de Registro:
   El suscriptor debe presentarse con el 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 con presencia física se cumple con la captura de datos biométricos según Resolución SICYT N° 11/2025.

Se puede obtener soporte por correo electrónico a la dirección revocacion@digilogix.com.ar o a info@digilogix.com.ar que se encuentra disponible las VEINTICUATRO (24) horas del día.

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

Se hace referencia al apartado 1.3.3.

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 o aplicación, 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 o aplicación, autorizado a tal fin, debe probar su carácter de suscriptor para la Política Única de Certificación de acuerdo a lo indicado en el apartado 1.3.3.

En el caso de la emisión de un certificado que no sea para una persona humana, toda la documentación que acredite su personería, acorde al punto 3.2, deberá haber sido analizada.

El solicitante deberá:

En caso de emisión en un dispositivo criptográfico:

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

b) Registrar una fotografía de su rostro y su huella dactilar según las Pautas Técnicas y de Procedimientos para la Toma de Datos Biométricos aprobadas por la Resolución SICYT N° 11/2025

c) Firmar el acuerdo con suscriptores

d) Abrir el correo electrónico enviado por la Autoridad de Registro donde se le presenta un link para poder crear una contraseña.

e) En el caso de que concurra a la Autoridad de Registro con su propio equipo portátil debe descargar e instalar la aplicación para suscriptores, de lo contrario usará los equipos disponibles en la misma. f) Ingresar al sitio web de DIGILOGIX S.A. https://suscriptor.digilogix.com.ar

g) Iniciar sesión con sus credenciales

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

i) Iniciará sesión en la aplicación.

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

k) 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

l) Esperar la aprobación y emisión del certificado.

m) 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 emisión en el Servicio de Firma Digital con Custodia Centralizada de claves criptográficas conforme la Resolución N° 86/20 de la ex Secretaría de Innovación Pública en modalidad presencia física:

Además, deberá contar con un teléfono celular que sea capaz de ejecutar el Autenticador de Google en su última versión.

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

b) Registrar una fotografía de su rostro y su huella dactilar según las Pautas Técnicas y de Procedimientos para la Toma de Datos Biométricos establecidas en la Resolución SICYT N° 11/2025 y se valida contra el Renaper.

c) Firmar el acuerdo con suscriptores

d) Abrir el correo electrónico enviado por la Autoridad de Registro donde se le presentan un link para poder crear una contraseña.

e) Iniciar sesión con sus credenciales en el sitio web de DIGILOGIX S.A. https://suscriptor.digilogix.com.ar/

f) Hacer click en el botón de “Nueva solicitud” en la página web.

g) La página web solicitará generar una relación a través del Autenticador de Google para disponer de una clave de un único uso (OTP) sin la cual no es posible hacer uso de la clave privada en custodia y un PIN asociada unívocamente al par de claves.

h) Revisar que sus datos sean correctos y enviar la solicitud a la Autoridad de Registro.

i) Esperar la aprobación, luego se genera el par de claves criptográficas en el dispositivo de Custodia Centralizada de claves criptográficas y se emite el certificado para poder hacer uso del mismo.

j) Se le envía un correo electrónico al suscriptor para informarle que el certificado digital ha sido emitido exitosamente.

El suscriptor dispondrá de un PIN por cada certificado emitido y una aplicación OTP en su celular vinculada a su identidad personal dentro de nuestros servidores.

A través de la web de suscriptores puede firmar un documento para lo cual necesitara todas las credenciales mencionadas anteriormente para autorizar la firma del mismo.

En caso de emisión en el Servicio de Firma Digital con Custodia Centralizada de claves criptográficas conforme Resolución N° 86/20 de la Secretaría de Innovación Pública en modalidad presencia telemática:

El proceso de emisión puede iniciarse mediante una computadora o desde un teléfono celular. En caso de utilizar una computadora, será necesario contar además con un teléfono celular con cámara frontal y posterior para completar las etapas de validación biométrica. Si el proceso se realiza íntegramente desde un teléfono celular, el mismo dispositivo podrá utilizarse para todas las etapas del procedimiento.

. Además, deberá contar con la capacidad de ejecutar el Autenticador de Google en su última versión.

a) Ingresar en https://onboarding.digilogix.com.ar/.
b) Ingresar en ”No tengo usuario” (en el caso de la primera emisión, de lo contrario ingresa con sus datos)
c) Ingresar el correo electrónico y el sistema le enviara un correo para iniciar el proceso de registración.
d) Ingresa a la URL enviada por correo electrónico y genera una contraseña
e) Ingresa nuevamente a https://onboarding.digilogix.com.ar con las credenciales generadas
f) Acepta los términos y condiciones
g) Cargar un medio de pago del que se cobrará la gestión.
h) Ingresando al link se procede a verificar la identidad del solicitante haciendo uso del servicio de RENAPER. Si ingresó desde una computadora personal, deberá continuar con los siguientes pasos desde un teléfono celular.
i) A continuación, se le solicitará tomar fotografías de frente y reverso del DNI.
j) Acto seguido se le tomará una fotografía del rostro.
k) Si la validación es exitosa, se reciben los datos del solicitante para ser mostrados y confirmados por el mismo.
l) A continuación, deberá crear el PIN para poder hacer luego uso de la firma digital. Se le informa al solicitante que, sin este dato, no podrá hacer uso la firma.

m) Se le solicitará generar una relación a través del Autenticador de Google para disponer de una clave de un único uso (OTP) sin la cual no es posible hacer uso de la clave privada en custodia.
n) Se le presenta el acuerdo con suscriptores y para firmar el mismo, se le solicitará el PIN y OTP recién generados.
o) Se le informa al suscriptor que la firma digital ha sido emitida.
p) El suscriptor dispondrá de un PIN por cada certificado emitido y una aplicación OTP vinculada a su identidad personal dentro de nuestros servidores.
Si la validación de la identidad con el RENAPER no fuera exitosa, debe habilitarse la contingencia para la validación de la identidad, en modalidad presencia física, con el número de trámite del DNI utilizando el servicio del Sistema de Identidad Digital (SID) que pone a disposición el mencionado Registro Nacional de las Personas.

A través de la web de suscriptores puede firmar un documento para lo cual necesitará todas las credenciales mencionadas anteriormente para autorizar la firma del mismo.

4.2.- Procesamiento de la solicitud del certificado

En el caso de la emisión con presencia física, 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 las Pautas Técnicas y de Datos de Procedimientos para la Toma de Datos Biométricos dispuestas por la Resolución SICYT N°11/2025, la AR efectúa una captura de fotografía y de la huella dactilar del solicitante del certificado utilizando un dispositivo biométrico, que luego se confronta utilizando los servicios de RENAPER..
- 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.

En el caso de la emisión con presencia telemática:

- Se pone a disposición del solicitante los Términos y Condiciones del servicio , el cual contiene una copia del acuerdo con suscriptores donde se deja constancia que para poner a disposición el certificado se debe firmar el acuerdo con suscriptores con firma digital.
- La validación de la identidad del solicitante se realiza mediante el confronte de la información suministrada y el servicio de validación de identidad que presta el RENAPER.
- Una vez validada la identidad del solicitante, se exhibe el Acuerdo con Suscriptores y se le solicita tanto OTP como pin para firmar el mismo.

- Emitido el certificado y puesto a disposición se notifica al suscriptor de la disponibilidad del mismo.

En ambos casos se 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.

Tanto en el supuesto de emisión con presencia física como en el de emisión del certificado de manera telemática, los Oficiales de Registro conservan la documentación de respaldo **en la base datos,** con toda la documentación recibida de los solicitantes o suscriptores de los certificados digitales.

4.3.- Emisión del certificado

4.3.1.- Proceso de emisión del certificado

Cumplidos los recaudos del proceso enunciado en el apartado 4.1.2. Solicitud de certificado y una vez aprobada la solicitud de certificado por la Autoridad de Registro correspondiente, la Autoridad Certificante **AC-DIGILOGIX** emitirá el certificado firmándolo digitalmente con su clave privada y lo pondrá a disposición del suscriptor.

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

4.3.2.- Notificación de emisión

Una vez cumplidos todos los pasos anteriores, la Autoridad de Registro la **AC-DIGILOGIX** emite el certificado firmándolo digitalmente y lo pone a disposición del suscriptor a través de la aplicación de suscriptores o a través del sitio web de suscriptores (www.digilogix.com.ar), y le comunica esa disponibilidad por correo electrónico.

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.

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

Según lo establecido en la Ley Nº 25.506, en su Artículo 25, el suscriptor debe:

a) Mantener el control exclusivo de sus datos de creación de firma digital, no compartirlos, e impedir su divulgación;
b) Utilizar UN (1) dispositivo de creación de firma digital técnicamente confiable;
c) Solicitar la revocación de su certificado al certificador ante cualquier circunstancia que pueda haber comprometido la privacidad de sus datos de creación de firma;

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

De acuerdo a lo establecido en la Resolución SICYT N° 11/2025 Anexo III, el suscriptor debe:

a) Resguardar y no divulgar aquellos factores de autenticación (contraseñas de usuario, OTP, PIN) que permitan utilizar la clave privada.

b) Proveer toda la información que le sea requerida a los fines de la emisión del certificado de modo completo y preciso.

c) Utilizar los certificados de acuerdo a lo establecido en la Política de Única Certificación.

d) Tomar debido conocimiento, a través del procedimiento previsto en cada caso, del contenido de la Política Única de Certificación, del Manual de Procedimientos, del Acuerdo con Suscriptores y de cualquier otro documento aplicable.

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

Se aplica el punto 3.3.2.- Generación de UN (1) certificado con el mismo par de claves.

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

En el caso de certificados digitales de Persona Humana o Jurídicas, la renovación del certificado posterior a su revocación o luego de su expiración requiere por parte del suscriptor el cumplimiento de los procedimientos previstos en el punto 3.2.3. - Autenticación de la identidad de Personas Humanas o lo previsto en el punto 3.2.2 - Autenticación de la identidad de Personas Jurídicas Públicas o Privadas Para los certificados de aplicaciones, incluyendo los de servidores, los responsables deben tramitar UN (1) nuevo certificado en todos los casos, cumpliendo los pasos requeridos en el apartado 3.2.2. Autenticación de la identidad de Personas Jurídicas Públicas o Privadas.

4.8.- Modificación del certificado

El suscriptor se encuentra obligado a notificar a **AC-DIGILOGIX** cualquier cambio en alguno de los datos contenidos en el certificado digital, que hubiera sido objeto de verificación, de acuerdo a lo dispuesto en el Inciso d) del Artículo 25 de la Ley N° 25.506. En cualquier caso, procede la revocación de dicho certificado y de ser requerido, la solicitud de uno nuevo.

4.9.- Suspensión y revocación de certificados

Los certificados serán revocados de manera oportuna y sobre la base de UNA (1) solicitud de revocación de certificado validada.

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

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, de la Resolución 182/19 y sus modificatorias, y Resolución SICYT Nº 11/2025 y sus normas reglamentarias.
- Ante incumplimiento por parte del suscriptor de la obligación de firmar el Acuerdo con Suscriptores.

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 SICYT N° 11/2025en 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:

a) Ingresando al sitio web de la AC – DIGILOGIX a la siguiente URL: https:// suscriptor.digilogix.com.ar/, utilizando los datos de acceso, es decir, el email registrado y la contraseña que estableció en el inicio del trámite. Una vez que el suscriptor ingresa a su portal, procederá a identificar el certificado a revocar, verificar sus datos y presionar REVOCAR, establecer el motivo y presionar nuevamente REVOCAR; en ese momento se le pide nuevamente la contraseña (PIN de revocación). Este sitio se encuentra disponible las VENTICUATRO (24) horas del día los SIETE (7) días de la semana, durante todo el año.

b) 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. En la revocación en forma

presencial se cumple con la captura de datos biométricos según lo establecido en la Resolución SICYT N° 11/2025 Anexo II Capítulo VII punto 7 e).
c) Presencia Telemática del suscriptor: validando los datos biométricos contra RENAPER.

4.9.4.- Plazo para la solicitud de revocación

El titular de un certificado debe requerir su revocación en forma inmediata cuando se presente alguna de las circunstancias previstas en el apartado 4.9.1.
El servicio de recepción de solicitudes de revocación se encuentra disponible en forma permanente SIETE POR VEINTICUATRO (7x24) horas cumpliendo con lo establecido en el Capítulo II Artículo 21 Incisos 8,9 y 10 del Decreto Nº 182/19.

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

El plazo máximo entre la recepción de la solicitud y el cambio de la información de estado del certificado indicando que la revocación ha sido puesta a disposición de los Terceros Usuarios, no superará en ningún caso las VEINTICUATRO (24) horas hábiles.

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/digilogixv3.crl

http://backup.digilogix.com.ar/ar/digilogixv3.crl

http://www.digilogix.com.ar/ar/digilogixv3+.crl

http://backup.digilogix.com.ar/ar/digilogixv3+.crl

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

Y además una página web de consultas online donde podrá buscar por Número de serie, CUIL/CUIT o Nombre:

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

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:// suscriptor.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.
  - http://www.digilogix.com.ar/ar/digilogixv3.crl
  - http://backup.digilogix.com.ar/ar/digilogixv3.crl
  - http://www.digilogix.com.ar/ar/digilogixv3+.crl
  - http://backup.digilogix.com.ar/ar/digilogixv3+.crl
- OCSP, permite verificar si el certificado se encuentra vigente o ha sido revocado.
  - http://ocspv3.digilogix.com.ar/ocsp
- WEB, permite verificar el estado de los certificados buscándolos por Número de serie, CUIL/CUIT o Nombre:
  - https://suscriptor.digilogix.com.ar/CertificadoSuscriptor/EstadosCertificados

4.10.2.- Disponibilidad del servicio

Los servicios se encuentran disponibles SIETE (7) x VEINTICUATRO (24) horas, sujetos a un razonable calendario de mantenimiento publicado en https://www.digilogix.com.ar/documentos .

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 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 la 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 este 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 SICYT N° 22/2025.

- 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 del 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. Protección lógica: el acceso es con dispositivos biométricos y el acceso al sistema operativo con 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:

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 Contingencia.

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 SICYT N° 11/2025 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 la 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 entonces 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 entonces Secretaría 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.

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 https://www.digilogix.com.ar

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 S.A.** 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.

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 es almacenado en el mismo dispositivo criptográfico FIPS 140-2 nivel 2 donde se genera, no permitiendo su exportación.
El par de claves privadas del Servicio de Firma Digital con Custodia Centralizada de Claves Criptográficas es almacenado en dispositivos criptográficos homologados FIPS 140-2 nivel 3.

6.2.7.- Almacenamiento de claves 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 SICYT N° 11/2025.

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

Para la desactivación de la clave privada de la **AC-DIGILOGIX** se aplican procedimientos que requieren la participación de los poseedores de las claves, según el control M de N. Para desarrollar esta actividad, los participantes son autenticados utilizando métodos adecuados de identificación.

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

Se entiende por datos de activación, a diferencia de las claves, a los valores requeridos para la operatoria de los dispositivos criptográficos y que necesitan estar protegidos.

Se establecen medidas suficientes de seguridad para proteger los datos de activación requeridos para la operación de los dispositivos criptográficos de los usuarios de certificados.

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.- 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.

El dispositivo criptográfico utilizado por **AC-DIGILOGIX** está certificado por el NIST (Nationa lInstitute of Standards and Technology) FIPS 140-2 Nivel 3 o superior.
Los dispositivos criptográficos utilizados por las Autoridades de Registro están certificados por NIST (National Institute of Standards and Technology) FIPS 140-2 Nivel 2 o superior.
Los dispositivos criptográficos utilizados por los suscriptores están certificados por NIST (National Institute of Standards and Technology) FIPS 140-2 Nivel 2 o superior.
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 o superior.

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

DIGILOGIX SA implementa procedimientos de control técnico para el ciclo de vida de los sistemas. Asimismo, se contemplan controles para el desarrollo, administración de cambios y gestión de la seguridad, en lo relacionado directa o indirectamente con las actividades de certificación.

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

En relación a los perfiles de los certificados, resulta de aplicación lo establecido en el apartado 7.1 de la Política Única de Certificación v.3.0.

7.2.- Perfil de la Lista de Certificados Revocados

Las listas de certificados revocados correspondientes a la Política Única de Certificación asociada a este Manual son emitidas conforme con lo establecido en la especificación ITU X.509 versión 2 y cumplen con las indicaciones establecidas en la sección “3 - Perfil de CRLs” del Anexo IV “Perfiles de los Certificados y de las Listas de Certificados Revocados” de la Resolución ex SIP N° 946/2021. En relación al perfil de la lista de certificados revocados, resulta de aplicación lo establecido en el apartado 7.2. de la Política Única de Certificación v.3.0.

7.3.- Perfil del Certificado del Servicio de Consulta OCSP

La consulta en línea del estado de un certificado digital se realiza utilizando el Protocolo OCSP (On-Line Certificate Status Protocol). Se implementa conforme a lo indicado en la especificación RFC 6960 “X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP” y cumple con las indicaciones establecidas en la Sección “4 - Perfil de la consulta en línea del estado del certificado” del Anexo IV “Perfiles de los Certificados y de las Listas de Certificados Revocados” de la Resolución SICYT N° 11/2025

7.3.1. Consultas OCSP

Los siguientes datos se encuentran presentes en las consultas:

• Versión (versión).

• Requerimiento de servicio (service request).

• Identificador del certificado bajo consulta (target certificate identifier).

• Extensiones opcionales (optional extensions), las cuales podrían ser procesadas por quien responde.

Al recibir la consulta OCSP, se determina:

• Si el formato de la consulta es adecuado.

• Si quien responde se encuentra habilitado para responder la consulta.

• Si la consulta contiene la información que necesita quien responde.

Si alguna de estas condiciones no se cumpliera, da lugar a un mensaje de error. De lo contrario se devuelve una respuesta.

7.3.2. Respuestas OCSP

Todas las respuestas OCSP son firmadas digitalmente por la Autoridad certificante de la **AC-DIGILOGIX** y contienen

los siguientes datos:

• Versión de la sintaxis de respuesta.

• Identificador de quien responde.

• Fecha y hora en la que se genera la respuesta.

• Respuesta respecto al estado del certificado.

• Extensiones opcionales.

• Identificador (OID) único del algoritmo de firma.

• Firma de la respuesta.

La respuesta a una consulta OCSP consiste en:

• Identificador del certificado.

• Valor correspondiente al estado del certificado.

• Período de validez de la respuesta.

• Extensiones opcionales. Se especifican las siguientes respuestas posibles para el valor correspondiente al estado

del certificado:

• Válido (good), indicando una respuesta positiva a la consulta. Este valor indica que no existe un certificado

digital con el número de serie contenido en la consulta, que haya sido revocado durante su vigencia.

• Revocado (revoked), indicando que el certificado ha sido revocado.

• Desconocido (unknown), indicando que quien responde no reconoce el número de serie incluido en la consulta,

debido comúnmente a la inclusión de un emisor desconocido.

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, CIENCIA Y TECNOLOGÍA dependiente de la JEFATURA DE GABINETE DE MINISTROS, en cumplimiento con la Resolución SICYT N° 11/2025.

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, CIENCIA y TECNOLOGÍA de la JEFATURA DE GABINETE DE MINISTROS.

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, podrá realizar 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 Artículos 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, su Decreto Reglamentario Nº 182/19, normas modificatorias y complementarias 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 S.A.**, en su carácter de certificador, garantiza la confidencialidad frente a terceros de su clave privada, la que, al ser el punto de máxima confianza, será generada y custodiada conforme a lo que se especifique en la Política 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 Plan de Contingencia, 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 SICYT N° 11/2025 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 Artículo 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: https://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 o conflicto derivado de la aplicación del presente Manual de Procedimientos deberá ser inicialmente canalizado mediante reclamo por escrito dirigido a DIGILOGIX S.A., en su carácter de Certificador Licenciado.

Recibido el reclamo, DIGILOGIX S.A. citará al reclamante a una audiencia, labrando acta con constancia de los hechos y antecedentes que motivan la presentación. El acta será notificada en forma fehaciente a las partes involucradas —Autoridad de Registro, Suscriptor y/o Tercero Usuario— quienes dispondrán de un plazo de DIEZ (10) días corridos para ofrecer prueba, formular alegaciones y ejercer su defensa.

Finalizado dicho plazo, DIGILOGIX S.A. emitirá resolución fundada dentro de los DIEZ (10) días corridos siguientes, conforme a criterios de razonabilidad, equidad y sujeción al marco normativo vigente.

En caso de disconformidad con lo resuelto o ante falta de respuesta dentro del plazo indicado, las partes podrán recurrir ante la Autoridad de Aplicación, conforme lo previsto en la Ley N.º 25.506, el Decreto N.º 182/2019 y sus modificatorios, y la Resolución SICYT N.º 11/2025.

Lo anterior se entiende sin perjuicio del derecho de las partes a acudir a la vía judicial competente.

En ningún caso el presente Manual de Procedimientos prevalecerá sobre lo dispuesto por la normativa legal vigente en materia 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, el Decreto N° 743/24, la Resolución SICYT N° 11/2025 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, el Decreto N° 743/24, la Resolución SICYT N° 11/2025 y 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	09/11/2022	Directorio DIGILOGIX	Renovación de licencia
Versión 3.0	26/08/2024	Directorio DIGILOGIX	Renovación de certificado
Versión 4.0	28/02/2025	Directorio DIGILOGIX	Adecuación al Decreto N° 743/24 y a la Resolución SICYT N° 11/2025

República Argentina - Poder Ejecutivo Nacional
AÑO DE LA RECONSTRUCCIÓN DE LA NACIÓN ARGENTINA

Hoja Adicional de Firmas
Anexo

Número: IF-2025-95380015-APN-SSI#JGM

CIUDAD DE BUENOS AIRES
Jueves 28 de Agosto de 2025

Referencia: Anexo II - Manual de Procedimientos V.4.0 - DIGILOGIX S.A.

El documento fue importado por el sistema GEDO con un total de 54 pagina/s.

Digitally signed by GESTION DOCUMENTAL ELECTRONICA - GDE
Date: 2025.08.28 15:47:09 -03:00

Claudio Gustavo WENDLER
Subsecretario
Subsecretaría de Innovación
Jefatura de Gabinete de Ministros

Digitally signed by GESTION DOCUMENTAL ELECTRONICA - GDE
Date: 2025.08.28 15:47:10 -03:00