POLÍTICA ÚNICA DE CERTIFICACIÓN

CERTIFICADOR LICENCIADO

DIGILOGIX S.A.

Versión 3.0

ÍNDICE

1- INTRODUCCIÓN.

1.1.- Descripción general

El presente documento establece las políticas que se aplican a la relación entre **AC – DIGILOGIX** en su carácter de Certificador Licenciado y los solicitantes, suscriptores, y terceros usuarios de los certificados que éste emita, en el marco de la Infraestructura de FirmaDigital de la REPÚBLICA ARGENTINA (Ley Nº 26.506 y sus modificatorias). Un certificado vincula los datos de verificación de firma digital de una persona humana o jurídica o con una aplicación a un conjunto de datos que permiten identificar a dicha entidad, conocida como suscriptor del certificado.

La Autoridad de Aplicación de la Infraestructura de firma digital es la SECRETARIA DE INNOVACION, CIENCIA Y TECNOLOGIA de la JEFATURA DE GABINETE DE MINISTROS, siendo dicho organismo y la SUBSECRETARIA DE INNOVACION, quienes entienden en las funciones de Ente Licenciante.

1.2.- Nombre e Identificación del Documento

a) Nombre: Política Única de Certificación de **DIGILOGIX S.A.**

b) Versión: 3.0

Fecha de aplicación: A partir de su aprobación por el Ente Licenciante

c) OID de la Política de Certificación: 2.16.32.1.1.7

d) Sitio de publicación: se publica en el sitio web de la **AC – DIGILOGIX**

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

e) Lugar: República Argentina

1.3.- Participantes

Integran la infraestructura del certificador las siguientes entidades:

1.3.1.- Certificador

Razón Social: DIGILOGIX S.A. 30-71412871-6

Domicilio: Rivadavia 789 Piso 4º Código Postal: C1002AAF

Ciudad Autónoma de Buenos Aires

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

Correo electrónico: info@digilogix.com.ar

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

1.3.2.- Autoridad de Registro

Las Autoridades de Registro de la **AC – DIGILOGIX** tienen por función la identificación y validación de identidad y de los otros datos de los solicitantes y suscriptores de certificados digitales que a su vez lleva implícita la tarea de verificación y guarda de la documentación respaldatoria presentada por los mismos.

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

a) Autoridad de Registro Central: Opera bajo la órbita directa de **AC – DIGILOGIX**, tiene dos formas, fija o móvil según Decreto N° 182/19 art. 31.

b) Autoridades de Registro Descentralizadas: funcionan en distintas organizaciones previa aprobación de **DIGILOGIX S.A.** Estas Autoridades de Registro operan bajo el estricto control y supervisión de la Autoridad de Registro Central de **DIGILOGIX S.A**.

Toda información vinculada a las Autoridades de Registro de la **AC – DIGILOGIX** se encuentra publicada en: https://www.digilogix.com.ar/Home/Contact según Resolución Nº 946/21 Anexo I Capítulo IV art. 27.

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 946/21 Anexo I Capítulo V art 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 presente Política Única de Certificación, toda persona humana o jurídica que recibe un documento firmado digitalmente y que genera una consulta para verificar la validez del certificado digital correspondiente, de acuerdo a la normativa vigente aplicable a la Firma Digital.

1.4. – Uso de los certificados

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

1.5. – Administración de la Política

1.5.1. – Organización administradora del documento

Es responsable de la presente Política Única de Certificación 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 de la Política Única de Certificación de **DIGILOGIX SA** es la máxima autoridad del Certificador Licenciado **AC – DIGILOGIX**:

Correo electrónico: info@digilogix.com.ar

Teléfono: +54 11 4345 5150 opción 4

Domicilio: Rivadavia 789 Piso 4º Código Postal: C1002AAF

Ciudad Autónoma de Buenos Aires

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

1.5.3. – Organismo encargado de aprobar la Política Única de Certificación

La Política Única de Certificación ha sido presentada ante la SUBSECRETARIA DE INNOVACION dependiente de la SECRETARIA DE INNOVACION, CIENCIA Y TECNOLOGIA de la JEFATURA DE GABINETE DE MINISTROS.

1.6. – Definiciones y Acrónimos

1.6.1. – Definiciones

- Autoridad de Aplicación: la SECRETARIA DE INNOVACION, CIENCIA Y TECNOLOGIA dependiente de la JEFATURA DE GABINETE DE MINISTROS es la Autoridad de Aplicación de firma digital en la REPUBLICA ARGENTINA.
- Autoridad de Registro: es la entidad que tiene a su cargo las funciones de:

- Recepción de las solicitudes de emisión de certificados.
- Validación de la identidad y autenticación de los datos de los titulares de certificados.
- Validación de otros datos de los titulares de certificados que se presenten ante ella cuya verificación delegue el Certificador Licenciado.
- Remisión de las solicitudes aprobadas al Certificador Licenciado con la que se encuentre operativamente vinculada.
- Recepción y validación de las solicitudes de revocación de certificados; y su direccionamiento al Certificador Licenciado con el que se vinculen.
- Identificación y autenticación de los solicitantes de revocación de certificados.
- Archivo y la conservación de toda la documentación respaldatoria del proceso de validación de identidad, de acuerdo con los procedimientos establecidos por el certificador licenciado.

- Cumplimiento de las normas y recaudos establecidos para la protección de datos personales.
- Cumplimiento de las disposiciones que establezca la Política de Certificación y el Manual de Procedimientos del Certificador Licenciado con el que se encuentre vinculada, en la parte que resulte aplicable.
- Cumplimiento con la Resolución 116/2017, establece la captura de fotografía digital del rostro y la huella dactilar de los solicitantes y suscriptores de firma digital.

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

- Certificado Digital: Se entiende por certificado digital al documento digital firmado digitalmente por un certificador, que vincula los datos de verificación de firma a su titular (Artículo 13 de la Ley N° 25.506).

- Certificador Licenciado: Se entiende por certificador licenciado a toda persona de existencia ideal, registro público de contratos u organismo público que expide certificados, presta otros servicios en relación con la firma digital y cuenta con una licencia para ello, otorgada por el ente licenciante. (Artículo 17 de la Ley N° 25.506).

- 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: SUBSECRETARIA DE INNOVACION y la SECRETARIA DE INNOVACION, CIENCIA Y TECNOLOGIA de la JEFATURA DE GABINETE DE MINISTROS.

- Lista de Certificado 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. Los certificados digitales que permitan identificar en forma fehaciente e internet o cualquier otra red informática, a los servidores que establezcan conexiones seguras, son también certificados de aplicaciones.
- 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 946/21 Anexo I Capítulo V art 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

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

NIST – NationalInstitute of Standards and Technology

OCSP – On Line Certificate Status Protocol

OID – Identificador de Objeto (“ObjectIdentifier”)

PKCS#10 – Public-Key Cryptography Standards

RFC – RequestforComments

RSA – Rivest, Shamir y Adleman

SHA – Secure Hash Algorithm

X509 – Estándar UIT-T para infraestructuras de claves públicas

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

Conforme a lo dispuesto por la Ley de Firma Digital N° 25.506, la relación entre **AC – DIGILOGIX** que emite un certificado digital y el titular de ese certificado se rige por el contrato que celebren entre ellos, sin perjuicio de las previsiones de la citada ley, y demás legislación vigente.

Al emitir un certificado digital o al reconocerlo en los términos del art. 16 de la Ley N° 25.506, **AC – DIGILOGIX** es responsable por los daños y perjuicios que provoque, por los incumplimientos a las previsiones de ésta, por los errores u omisiones que presenten los certificados digitales que expida, por no revocarlos, en legal tiempo y forma cuando así correspondiere y por las consecuencias imputables a la inobservancia de procedimientos de certificación exigibles todo ello de acuerdo con los establecido en el art. 38 de la Ley N° 25.506.

El Art. 32 del Decreto Nº182/19, reglamentario de la Ley Nº 25.506, establece la responsabilidad del Certificador respecto de las AR.

AC – DIGILOGIX es responsable con los alcances establecidos en la Ley N° 25.506, aún en el caso de que delegue parte de su operatoria en una AR, sin perjuicio del derecho de **AC – DIGILOGIX** de reclamar a la AR las indemnizaciones por los daños y perjuicios que aquél sufriera como consecuencia de los actos y/u omisiones de ésta.

AC – DIGILOGIX tampoco es responsable en los siguientes casos, según el Art. 39 de la Ley antes mencionada:

a) Por los casos que se excluyan taxativamente en las condiciones de emisión yutilización de sus certificados digitales y que no estén expresamente previstos en la Ley N° 25.506;

b) Por los daños y perjuicios que resulten del uso no autorizado de un certificado digital, si en las correspondientes condiciones de emisión y utilización de sus certificados constan las restricciones de su utilización;

c) Por eventuales inexactitudes en el certificado que resulten de la información facilitada por el titular que, según lo dispuesto en las normas y en los manuales de procedimientos respectivos, deba ser objeto de verificación, siempre que **AC – DIGILOGIX** pueda demostrar que ha tomado todas las medidas razonables.

La AR siempre exigirá la presencia física del suscriptor, la captura de la fotografía del rostro y la huella dactilar como así también la documentación correspondiente. Todos los trámites realizados por las Autoridades de Registro son firmados digitalmente por los oficiales de registro y operadores que los realizan, asumiendo así su plena responsabilidad en el proceso. Los alcances de la responsabilidad de **AC – DIGILOGIX** se limitan a las consecuencias directas de la falta de cumplimiento de los procedimientos establecidos en esta Política Única de Certificación en relación a la emisión, renovación y revocación de certificados. Los alcances de la responsabilidad **AC – DIGILOGIX** se limitan a los ámbitos de su incumbencia directa, en ningún momento será responsable por el mal uso de los certificados que pudiera hacerse, tampoco por los daños y perjuicios derivados de la falta de consulta de la información disponible en Internet sobre la validez de los certificados, ni tampoco será responsable de losusos de los certificados en aplicaciones específicas.

AC – DIGILOGIX no garantiza el acceso a la información cuando mediaran razones de fuerza mayor (catástrofes naturales, cortes masivos de luz por períodos indeterminados, destrucción debido a eventos no previstos, etc.) ni asume responsabilidad por los daños o perjuicios que se deriven en forma directa o indirecta como consecuencia de estos casos.

2.1. – Repositorios

El servicio de repositorio de información y la publicación de la Lista de Certificados Revocados son administrados en forma directa por **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:

- Política Única de Certificación anteriores y vigente
- Acuerdo con Suscriptores
- Términos y condiciones con Terceros Usuarios
- Política de Privacidad
- Manual de Procedimientos (parte pública)
- Información relevante de los informes de su última auditoría
- Repositorio de certificados revocados
- Certificados del Certificador Licenciado y acceso al de la Autoridad Certificante Raíz
- Consulta de certificados emitidos (indicando su estado). Se pueden consultar en: https://www.digilogix.com.ar/CertificadoSuscriptor/EstadosCertificados
- Listado de AR. Se puede consultar en: https://www.digilogix.com.ar/Home/Contact

La lista de Certificados Revocados (CRL) en: http://www.digilogix.com.ar/ar/digilogixv3.crl y 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**.

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

2.3. – Frecuencia de publicación

Se garantiza la actualización inmediata del repositorio cada vez que cualquiera de los documentos publicados sea modificado.

2.4. – Controles de acceso a la información

Se garantizan los controles de los accesos al certificado de **AC – DIGILOGIX**, a la Lista de Certificados Revocados y a las versiones anteriores y actualizadas de la Política de Certificación y a su Manual de Procedimientos (excepto en sus aspectos confidenciales).

Solo se revelará información confidencial o privada, si es requerida judicialmente o en el marco de procedimientos administrativos.

En virtud de lo dispuesto por la Ley de Protección de Datos Personales N° 25.326 y por el inciso h) del Art. 21 de la Ley N° 25.506, el solicitante o titular de un certificado digital podrá solicitar el acceso a toda la información relativa a las tramitaciones realizadas.

DIGILOGIX S.A. garantiza el acceso permanente, irrestricto y gratuito a la información publicada en su repositorio.

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]"

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

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

  b. En caso de extranjeros: "PA" [país]: Número de Pasaporte y código de país emisor. El atributo [país] esta codificado según el estándar [ISO3166] de DOS (2) caracteres. "EX" [país]: Número y tipo de documento extranjero aceptado en virtud de acuerdos internacionales. El atributo [país] esta codificado según el estándar [ISO3166] de DOS (2) caracteres.
- "*countryName*" (OID 2.5.4.6: Código de país): Esta presente y representa el país de emisión de los certificados, codificado según el estándar [ISO3166] de DOS (2) caracteres.

Para los certificados de Personas Jurídicas Públicas o Privadas:

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

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

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

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

  a. “CUIT”: Clave Única de Identificación Tributaria para las Personas Jurídicas argentinas.

  b. “ID” [país]: Número de identificación tributario para Personas Jurídicas extranjeras. El atributo [país] esta codificado según el estándar [ISO3166] de 2 caracteres.
- “countryName” (OID 2.5.4.6: Código de país): Esta presente y representa el país de emisión de los certificados, codificado según el estándar [ISO3166] de 2 caracteres.

Para los Certificados de Autoridad de Sello de Tiempo:

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

respetando el siguiente formato y codificación: “[código de identificación]” “[nro. De identificación]”

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

a. “CUIT”: Clave Única de Identificación Tributaria para las Personas Jurídicas argentinas.

b. “ID” [país]: Número de identificación tributaria para Personas Jurídicas extranjeras.

El atributo [país] DEBE estar codificado según el estándar [ISO 3166] de DOS (2) caracteres.

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

Para los Certificados de Autoridad de Sello de Competencia:

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

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

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

3.1.3. – Anonimato o uso de seudónimos

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

3.1.4. – Reglas para la interpretación de nombres

Todos los nombres representados dentro de los certificados emitidos bajo la presente Política coinciden con los correspondientes al documento de identidad del suscriptor o con la documentación presentada por la Persona Jurídica. Las discrepancias o conflictos quepuedan 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 uncertificado 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 depersonas 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

Se describen los procedimientos a utilizar para autenticar, como paso previo a la emisión de UN (1) certificado, la identidad y demás atributos del solicitante que se presente ante **AC – DIGILOGIX** o ante la Autoridad de Registro operativamente vinculada. Se establecen los medios admitidos para recibir los requerimientos de certificados y para comunicar su aceptación.

AC – DIGILOGIX cumple con lo establecido en:

- Ley de Firma Digital Nº 25.506 y el art. 21 punto 7 del Anexo al Decreto Reglamentario 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, la cual no incluye dicha clave. Las claves siempre son generadas por el solicitante. En ningún caso **AC – DIGILOGIX** ni sus autoridades de registro podrán tomar conocimiento o acceder bajo ninguna circunstancia a las claves de los solicitantes o titulares de los certificados, conforme el inciso b) del artículo 21 de la Ley N° 25.506.

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

3.2.2 – Autenticación de la identidad de Personas Jurídicas Públicas o Privadas

Los procedimientos de autenticación de la identidad de los suscriptores de los certificados de Personas Jurídicas Públicas o Privadas comprenden los siguientes aspectos:

a) El requerimiento debe efectuarse únicamente por intermedio del responsable autorizado a actuar en nombre del suscriptor para el caso de certificados de Personas Jurídicas o de quien se encuentre a cargo del servicio, aplicación o sitio web.

b) **AC – DIGILOGIX** o la autoridad del registro, en su caso, verificará la identidad del responsable antes mencionado y su autorización para gestionar el certificado correspondiente.

c) El responsable mencionado en el apartado a) validará su identidad según lo dispuesto en el apartado siguiente.

d) La identidad de la Persona Jurídica titular del certificado o responsable del servicio, aplicación o sitio web es verificada mediante documentación que acredite su condición de tal. La documentación a presentarse según sea el solicitante o suscriptor, será la siguiente:

Para Personas Jurídicas Públicas o Privadas:

a) Documento de identidad (original y fotocopia) del responsable autorizado
b) Acuerdo con Suscriptores firmado
c) Recibo que acredita el pago del certificado correspondiente

De tratarse de Personas Jurídicas Privadas, registro con los documentos que se detallan más abajo con copias certificadas por Escribano Público de corresponder:

a) Estatuto o Contrato Social correspondiente a la Persona Jurídica o documento análogo
b) Poder General Amplio, Acta de directorio o Poder Especial que autorice la solicitud de certificado de firma digital
c) Constancia de inscripción en el Registro Público de Comercio o documento análogo

d) Constancia de inscripción en AFIP

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

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

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

AC – DIGILOGIX cumple con las siguientes exigencias reglamentarias impuestas por:

a) El art. 21, inciso i) de la Ley Nº 25.506 relativo a la conservación de la documentación de respaldo de los certificados emitidos.

b) El art. 21, inciso f) de la Ley Nº 25.506 relativo a la recolección de datos personales.

c) El art. 21, inciso 14, Capítulo II del Decreto Nº 182/19 relativo a la protección de datos personales.

Debe conservarse la documentación que respalda el proceso de identificación de la persona responsable de la custodia de las claves criptográficas.

El responsable autorizado o a cargo del servicio, aplicación o sitio web debe firmar UN (1) acuerdo que contenga la confirmación de que la información incluida en el certificado es correcta.

En concordancia con la Resolución N° 116/2017, **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.

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.

- Se exige la presencia física del solicitante o suscriptor del certificado ante **AC – DIGILOGIX** o la Autoridad de Registro con la que se encuentre operativamente vinculado y se cumple con lo establecido en la Resolución N° 116/2017. La verificación se efectúa mediante la presentación de los siguientes documentos:
- De poseer nacionalidad argentina, se requiere Documento Nacional de Identidad.
- De tratarse de extranjeros, se requiere Documento Nacional de Identidad argentino o Pasaporte válido u otro documento válido aceptado en virtud de acuerdos internacionales.

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

Se consideran obligatorias las exigencias reglamentarias impuestas por:

a) El art. 21, inciso i) de la Ley Nº 25.506 relativo a la conservación de la documentación de respaldo de los certificados emitidos.

b) El art. 21, inciso f) de la Ley Nº 25.506 relativo a la recolección de datos personales.

c) El art. 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 art. 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. 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.

3.2.4. – Información no verificada del suscriptor

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

3.2.5. – Validación de autoridad

Según lo dispuesto en el punto 3.2.2., **AC – DIGILOGIX** o la Autoridad de Registro con la que se encuentre operativamente vinculado, verifica la autorización de la Persona Humana que actúa en nombre de la Persona Jurídica para gestionar el certificado correspondiente.

3.2.6. – Criterios para la 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 nuevo par de claves (Rutina de Re Key)

3.3.1. – Renovación con generación de nuevo par de claves (Rutina de Re Key)

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.

Si la solicitud del nuevo certificado se realiza antes de la expiración del certificado no se exigirá la presencia física debiendo el solicitante remitir la constancia firmada digitalmente del inicio del trámite de renovación.

La renovación sin presencia física del certificado se podrá realizar una sola vez.

3.3.2. – Generación de UN (1) certificado con el mismo par de claves

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

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

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

3.4. – Requerimiento de revocación

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

Los suscriptores o las personas autorizadas podrán pedir la revocación del certificado a través de alguno de los siguientes medios:

a) Por correo electrónico firmado digitalmente a las direcciones: revocacion@digilogix.com.ar o a info@digilogix.com.ar que se encuentra disponible las VEINTICUATRO (24) horas del día.

b) Ingresando al sitio web de la **AC – DIGILOGIX** a la siguiente URL: https://www.digilogix.com.ar/suscriptor, utilizando los datos de acceso que le fuera

informado por email al momento de la emisión de su certificado. Una vez que el suscriptor ingresa a su portal con sus datos de acceso debe ingresar a la solapa CERTIFICADOS, verificar sus datos y presionar REVOCAR, establecer el motivo y presionar nuevamente REVOCAR en ese momento se le pide el PIN de revocación.

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

4. - CICLO DEL CERTIFICADO: REQUERIMIENTOS OPERATIVOS

4.1. - Solicitud de certificado

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, aplicación o sitio web, autorizado a tal fin, en el caso de Personas Jurídicas.

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

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

El solicitante deberá:

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 Resolución N° 116/17.

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

f) Iniciar sesión con sus credenciales

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

h) 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.

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 Resolución N° 86/20 de la entonces Secretaría de Innovación Pública:

Las estaciones de trabajo de los solicitantes/suscriptores de certificados deben poseer Edge versión 76 o superior, Google Chrome 70 o superior, Mozilla Firefox 62 o superior.

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 Resolución N° 116/17.

c) Firmar el acuerdo con suscriptores

d) Abrir el correo electrónico enviado por la Autoridad de Registro donde se le presentan 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 atreves 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. Se genera el par de claves criptográficas en el dispositivo de Custodia Centralizada de claves criptográficas.

i) Esperar la aprobación y emisión del certificado para poder hacer uso del mismo.

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. Para poder generar la solicitud de emisión de certificado, ya sea de persona física o de persona jurídica, se le solicita al suscriptor que presente la misma documentación detallada en la política única de certificación (3.2.2 - Autenticación de la identidad de Personas Jurídicas Públicas o Privadas) (3.2.3. - Autenticación de la identidad de Personas Humanas)

4.2. - Procesamiento de la solicitud del certificado

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

- Valida la identidad del solicitante o su representante autorizado mediante la verificación de la documentación requerida y el cumplimiento de la Resolución N° 116/17, la AR efectúa una captura de fotografía y de la huella dactilar del solicitante del certificado utilizando un dispositivo biométrico.
- Requiere al solicitante o su representante autorizado la firma del Acuerdo con Suscriptores en su presencia con lo que quedan aceptadas las condiciones de emisión y uso del certificado digital.

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

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

Cumplidos los recaudos del proceso de validación de identidad y otros datos del solicitante, de acuerdo con esta Política Única de Certificación y una vez aprobada la solicitud de certificado por 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, 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 art. 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 N° 946/21 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.

Las claves pueden ser generadas a través de un servicio de custodia centralizada de claves criptográficas conforme Resolución N° 86/20 de la entonces Secretaría de Innovación Pública en este caso éste deberá estar integrado con los servicios de la Autoridad Certificante del Certificador Licenciado, cumpliendo los requisitos de seguridad de la información que permiten resguardar contra la posibilidad de intrusión y uno no autorizado.

4.5.2. - Uso de la clave pública y del certificado por parte de Terceros Usuarios

Los Terceros Usuarios deben:

a) Conocer los alcances de la presente Política Única de Certificación;

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, 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.

Si la solicitud de UN (1) nuevo certificado se realiza antes de la expiración del anterior, no habiendo sido este revocado, no se exigirá la presencia física, debiendo el solicitante remitir la constancia firmada digitalmente del inicio del trámite de renovación.

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 art. 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, sus normas reglamentarias.

AC - DIGILOGIX, de corresponder, revocará el certificado en un plazo no superior a las VEINTICUATRO (24) horas de recibido el requerimiento de revocación.

4.9.2. - Autorizados a solicitar la revocación

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

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

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

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

d) El Certificador o la Autoridad de Registro.

e) El Ente Licenciante.

f) La autoridad judicial.

g) La Autoridad de Aplicación.

4.9.3. - Procedimientos para la solicitud de revocación

AC - DIGILOGIX garantiza que:

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

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

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

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

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

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

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

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

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

4.9.4. - Plazo para la solicitud de revocación

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 art. 21 inciso 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.

4.9.6. - Requisitos para la verificación de la Lista de Certificados Revocados

Los Terceros Usuarios deben validar el estado de los certificados, mediante el control de la Lista de Certificados Revocados, a menos que utilicen otro sistema con características de seguridad y confiabilidad por lo menos equivalentes.

Los 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.

El certificador cumple con lo establecido en el Capítulo II art. 21, inciso 9 del Decreto Reglamentario Nº 182/19 relativo al acceso al repositorio de certificados revocados y las obligaciones establecidas en la Resolución 946/21 y sus correspondientes Anexos.

4.9.7. - Frecuencia de emisión de listas de certificados revocados

AC – DIGILOGIX genera y publica una Lista de Certificados Revocados asociada a esta Política Única de Certificación 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

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

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

Se utiliza el protocolo OCSP que permite, mediante su consulta, determinar el estado de un certificado digital y es una alternativa al servicio de CRLs, el que también estará disponible. Este servicio es accedido a través del sitio web http://ocspv3.digilogix.com.ar/ocsp. La respuesta de la consulta estará firmada con la clave del certificado OCSP correspondiente.

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

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

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

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

4.9.12. - Requisitos específicos para casos de compromiso de claves

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

4.9.13. - Causas de suspensión

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

4.9.14. - Autorizados a solicitar la suspensión

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

4.9.15. - Procedimientos para la solicitud de suspensión

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

4.9.16. - Límites del periodo de suspensión de un certificado

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

4.10. – Estado del certificado

4.10.1. – Características técnicas

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

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

4.10.2. – Disponibilidad del servicio

Ambos servicios se encuentran disponibles SIETE (7) x VEINTICUATRO (24) horas, sujetos a un razonable calendario de mantenimiento.

4.10.3. – Aspectos operativos

No existen otros aspectos a mencionar.

4.11. – Desvinculación del suscriptor

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

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

4.12. – Recuperación y custodia de claves privadas

En virtud de lo dispuesto en el inciso b) del art. 21 de la Ley N° 25.506, **AC – DIGILOGIX** se obliga a no realizar bajo ninguna circunstancia la recuperación o custodia de claves privadas de los titulares de certificados digitales. Asimismo, de acuerdo a lo dispuesto en el inciso a) del art. 25 de la ley citada, el suscriptor de un certificado emitido en el marco de esta Política

Única de Certificación se encuentra obligado a mantener el control exclusivo de su clave privada, no compartirla e impedir su divulgación.

5. - CONTROLES DE SEGURIDAD FÍSICA, OPERATIVOS Y DE GESTIÓN

Se describen a continuación los procedimientos referidos a los controles de seguridad física, de gestión y operativos implementados por **AC – DIGILOGIX**. La descripción detallada se encuentra en el Plan de Seguridad.

5.1. - Controles de seguridad física

- Se cuenta con controles de seguridad relativos a:

a) Construcción y ubicación de instalaciones

b) Niveles de acceso físico.

c) Comunicaciones, energía y ambientación.

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.

5.2. - Controles de Gestión

- Se cuenta con controles de seguridad relativos a:

a) Definición de roles afectados al proceso de certificación.

b) Número de personas requeridas por función.

c) Identificación y autenticación para cada rol.

d) Separación de funciones.

5.3. - Controles de seguridad del personal

a) Calificaciones, experiencia e idoneidad del personal, tanto de aquellos que cumplen funciones críticas como de aquellos que cumplen funciones administrativas, de seguridad, limpieza, etcétera.

b) Antecedentes laborales.

c) Entrenamiento y capacitación inicial.

d) Frecuencia de procesos de actualización técnica.

e) Frecuencia de rotación de cargos.

f) Sanciones a aplicar por acciones no autorizadas.

g) Requisitos para contratación de personal.

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

5.4. - Procedimientos de Auditoría de Seguridad

Se mantienen políticas de registro de eventos, cuyos procedimientos detallados son desarrollados en el Manual de Procedimientos.

Se cuenta con procedimientos de auditoría de seguridad sobre los siguientes aspectos:

a) Tipo de eventos registrados. Se cumple lo establecido en el Anexo II Sección 3 de la Resolución N° 946/21.

b) Frecuencia de procesamiento de registros.

c) Período de guarda de los registros. Debe respetarse lo establecido en el inciso i) del art. 21 de la Ley N° 25.506 respecto a los certificados emitidos.

d) Medidas de protección de los registros, incluyendo privilegios de acceso.

e) Procedimientos de resguardo de los registros.

f) Sistemas de recolección y análisis de registros.

g) Notificaciones del sistema de recolección y análisis de registros.

h) Evaluación de vulnerabilidades.

5.5. - Conservación de registros de eventos

Se han desarrollado e implementado políticas de conservación de registros, cuyos procedimientos detallados se encuentran desarrollados en el Manual de Procedimientos.

Los procedimientos cumplen con lo establecido por el art. 21, inciso i) de la Ley Nº 25.506 relativo al mantenimiento de la documentación de respaldo de los certificados digitales emitidos.

Se respeta lo establecido en el Anexo II Sección 3 de la Resolución 946/21 respecto del registro de eventos.

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

a) Tipo de registro archivado.

b) Período de guarda de los registros.

c) Medidas de protección de los registros archivados, incluyendo privilegios de acceso.

d) Procedimientos de resguardo de los registros.

e) Sistemas de recolección y análisis de registros

f) Procedimientos para obtener y verificar la información archivada.

5.6. - Cambio de claves criptográficas

El par de claves criptográficas 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 a 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 se encuentran desarrollados en el Plan de Continuidad de las Operaciones.

Se han desarrollado procedimientos referidos a:

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

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

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

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

Los procedimientos cumplen con lo establecido por el art. 20 del Decreto Nº 182/19 art. 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 182/19, 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 946/21 y sus correspondientes Anexos.

6. - CONTROLES DE SEGURIDAD TÉCNICA

Se describen las medidas de seguridad implementadas por **AC – DIGILOGIX** para proteger las claves criptográficas y otros parámetros de seguridad críticos. Además, se incluyen los controles técnicos que se implementan sobre las funciones operativas de **AC – DIGILOGIX**, Autoridades de Registro y suscriptores.

6.1. - Generación e instalación del par de claves criptográficas

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

a) Responsables de la generación de claves.

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

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

d) Características y tamaños de las claves.

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

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

6.1.1. - Generación del par de claves criptográficas.

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

- Por software, en este caso, las claves deben ser resguardadas con un PIN de seguridad para su acceso. Conforme al art 5 de la Resolución de la 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.

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 la Firma Digital de los suscriptores (incluyendo los roles vinculados a las actividades de registro), establecido por la Ley Nº 25.506, art. 21, inciso b) y el Decreto Nº 182/19, art. 21, punto 3).

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

Todo solicitante de un certificado emitido bajo esta Política Única de Certificación entrega su clave pública a la **AC – DIGILOGIX**, a través de la aplicación correspondiente, durante el proceso de solicitud del certificado.

La **AC – DIGILOGIX** utiliza técnicas de prueba de posesión para determinar que el solicitante se encuentra en posesión de la clave privada asociada a dicha clave pública.

Los procesos de solicitud utilizan el formato PKCS#10 para implementar la “prueba de

posesión", remitiendo los datos del solicitante y su clave pública dentro de una estructura firmada con su clave privada.

El procedimiento descripto asegura que:

- La clave pública no pueda ser cambiada durante la transferencia.
- Los datos recibidos por **AC – DIGILOGIX** se encuentran vinculados a dicha clave pública
- El remitente posee la clave privada que corresponde a la clave pública transferida.

6.1.4. - Disponibilidad de la clave pública del certificador

El certificado de la **AC – DIGILOGIX y** el de la Autoridad Certificante Raíz de la REPÚBLICA ARGENTINA (ACR-RA) y el resto de aquellos que compongan su cadena de certificación se encuentran a disposición de los suscriptores y terceros usuarios en su sitio web (http://www.digilogix.com.ar/documentacion)

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 Tiempopara 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 indican en el punto 6.1.5.

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

Las claves criptográficas de los suscriptores de los certificados pueden ser utilizados para firmar digitalmente, para funciones de autenticación y para cifrado.

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

La protección de la clave privada, considerada en este punto, se aplica para la Autoridad Certificante de **DIGILOGIX SA**, las Autoridades de Registro y los suscriptores.

Para cada una de estas entidades se abordan los siguientes temas:

a) Estándares utilizados para la generación del par de claves.

b) Número de personas involucradas en el control de la clave privada.

c) En caso de existir copias de resguardo de la clave privada, controles de seguridad establecidos sobre ellas.

d) Procedimiento de almacenamiento de la clave privada en un dispositivo criptográfico.

e) Responsable de activación de la clave privada y acciones a realizar para su activación.

f) Duración del período de activación de la clave privada y procedimiento a utilizar para su desactivación.

g) Procedimiento de destrucción de la clave privada.

h) Requisitos aplicables al dispositivo criptográfico utilizado para el almacenamiento de las claves privadas.

6.2.1. – Controles y estándares para dispositivos criptográficos

El dispositivo criptográfico utilizado por **AC – DIGILOGIX** está certificado por el NIST (National Institute of Standards and Technology) sobre la base del Estándar FIPS 140-2 Nivel 3.

Los dispositivos criptográficos utilizados por las AR están certificados por NIST

(NationalInstitute of Standards and Technology) sobre la base del Estándar FIPS 140-2 Nivel 2.

Los dispositivos criptográficos utilizados por suscriptores están certificados por NIST (NationalInstitute of Standards and Technology) sobre la base del Estándar FIPS 140-2 Nivel 2.

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

Los controles empleados para la activación de las claves se basan en la presencia de M de N con M mayor a 2.

6.2.3. - Recuperación de clave privada

Ante una situación que requiera recuperar su clave privada, y siempre que ésta no se encuentre comprometida, **AC – DIGILOGIX** cuenta con procedimientos para su recuperación. Estos procedimientos sólo pueden ser realizados por personal autorizado, sobre dispositivos criptográficos seguros y exclusivamente en el nivel de seguridad donde se realicen las operaciones críticas de la **AC – DIGILOGIX.**

No se implementan mecanismos de resguardo y recuperación de las claves privadas de las Autoridades de Registro y de los suscriptores. Estos deberán proceder a la revocación del certificado y a tramitar una nueva solicitud de emisión de certificado, si así correspondiere.

6.2.4. - Copia de seguridad de la clave privada

AC – DIGILOGIX genera una copia de seguridad de la clave privada a través de un procedimiento que garantiza su integridad y confidencialidad por personal autorizado de **DIGILOGIX SA** y almacenadas en dispositivos criptográficos seguros validados FIPS 140-2 nivel 3. Estos dispositivos son resguardados en un lugar de acceso restringido.

No se mantienen copias de las claves privadas de los suscriptores de certificados ni de los Oficiales de Registro.

6.2.5. - Archivo de clave privada

AC – DIGILOGIX almacena las copias de resguardo de su clave privada a través de un procedimiento que garantiza su integridad, disponibilidad y confidencialidad, conservándola en un lugar seguro, al igual que sus elementos de activación, bajo los niveles de seguridad requeridos por la normativa vigente de acuerdo a lo dispuesto por la Resolución N° 946/21 en cuanto a los niveles de resguardo de claves.

6.2.6. - Transferencia de claves privadas en dispositivos criptográficos

El par de claves criptográficas de **AC – DIGILOGIX** se genera y almacena en dispositivos criptográficos conforme a lo establecido en la presente Política, salvo en el caso de las copias de resguardo que también están soportados en dispositivos criptográficos homologados FIPS 140-2 nivel 3.

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

6.2.7. - Almacenamiento de claves privadas en dispositivos criptográficos

El almacenamiento de las claves criptográficas del **AC - DIGILOGIX** 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 respetando los niveles de seguridad física de acuerdo a lo establecido en la Resolución N° 946/21.

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

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

6.2.8. - Método de activación de claves privadas

Para la activación de la clave privada de la **AC - DIGILOGIX** se aplican procedimientos que requieren la participación de los poseedores de claves de activación según el control M de N. Estos participantes son autenticados utilizando métodos adecuados de identificación.

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 destruirán los dispositivos de soporte de su clave privada mediante un procedimiento que garantice su destrucción total y segura según el último estado del arte disponible a la fecha.

La clave privada de la **AC – DIGILOGIX** empleada para emitir certificados según los lineamientos de esta Política se utiliza 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 los Oficiales de Registro 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

Los certificados emitidos por la **AC - DIGILOGIX** y aquellos emitidos a los Oficiales de Registros de las Autoridades de Registro como así también el propio son almacenados bajo un esquema de redundancia y respaldados en forma periódica sobre dispositivos habilitados sólo para lectura, lo que, sumado a la firma de los mismos, garantiza su integridad.

Los certificados son almacenados en soporte magnético en formato estándar bajo codificación internacional DER.

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 **AC – DIGILOGIX** establece medidas de seguridad para proteger adecuadamente los datos de activación de la clave privada de los suscriptores de certificados contra usos no autorizados capacitándolos para el uso seguro y resguardo de los dispositivos correspondientes.

6.4.3. - Otros aspectos referidos a los datos de activación

La **AC – DIGILOGIX** establece 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. e induciendo a la elección de contraseñas fuertes para la protección de las claves privadas y para el acceso a dispositivos criptográficos si estos fueran utilizados.

6.5. - Controles de seguridad informática

6.5.1. - Requisitos Técnicos específicos

Se establecen los requisitos de seguridad referidos al equipamiento y al software del Certificador, cuyo detalle se encuentra en el Manual de Procedimientos.

Dichos requisitos se vinculan 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 productos en los que se basa la implementación de **DIGILOGIX S.A.** cumplen con los siguientes requisitos de seguridad:

Windows 2012 R2 Server: Common Criteria v3.1 R4

SQL 2012 x64: certificado EAL4+

El dispositivo criptográfico utilizado por **AC – DIGILOGIX** está certificado por el NIST con FIPS 140-2 Nivel 3 o superior.

Los dispositivos criptográficos utilizados por las Autoridades de Registro están certificados por NIST con FIPS 140-2 Nivel 2 o superior.

Los dispositivos criptográficos utilizados por los suscriptores están certificados por NIST con FIPS 140-2 Nivel 2 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

AC – DIGILOGIX cumple con procedimientos específicos para el diseño, desarrollo y prueba

de los sistemas entre los que se encuentran:

- Separación de ambientes de desarrollo, prueba y producción.
- Control de versiones para los componentes desarrollados.
- Pruebas con casos de uso.

6.6.2. – Controles de gestión de seguridad.

Se documenta y controla la configuración del sistema, así como toda modificación o actualización, habiéndose implementado un método de detección de modificaciones no autorizadas.

AC – DIGILOGIX cumple con la separación de ambientes de desarrollo, prueba y producción. Asimismo, cumple con el control de versiones para los componentes desarrollados y formaliza pruebas de uso.

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

No aplicable

6.7. - Controles de seguridad de red

Los servicios que provee **AC – DIGILOGIX** que se encuentran conectados a una red de comunicación pública, son protegidos por la tecnología apropiada que garantiza su seguridad.

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.

6.9 – Servicio de emisión de Sello de Competencia y/o Atributo

El servicio de emisión de sello de competencia de la **AC - DIGILOGIX** está basado en la especificación de los estándares

RFC 5755 “An Internet Attribute Certificate Profile for

Authorization”.

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

7.1. - Perfil del certificado

Todos los certificados serán emitidos conforme con lo establecido en la especificación ITU X.509 versión 3 (ISO/IEC 9594-8) “Information Technology – The Directory Public key and atribute certificate frameworks” adoptada como estándar tecnológico para la Infraestructura de Firma Digital de la REPÚBLICA ARGENTINA por la Resolución Nº 946/2021 Anexo IV.

AC – DIGILOGIX adhiere a las recomendaciones de los siguientes documentos en relación al perfil de los certificados:

- RFC 3739 “Internet X.509 Public Key Infrastructure Qualified Certificates Profile” [RFC3739].
- RFC 5280 “Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile” [RFC5280].

Los perfiles que se describen en este apartado corresponden a certificados y listas de Certificados Revocados emitidos con la cadena de certificación de la AC Raíz 2016.

Los perfiles que corresponden a la cadena de certificación de la AC Raíz 2007 se encuentran disponibles en la Política Única de Certificación de la **AC – DIGILOGIX** versión 2.0.

a) Perfil del certificado de Persona Humana

Certificado x.509 v3 Atributos Extensiones	Valor/OID	Contenido
Versión	Version	2 Corresponde a versión 3
Número de serie	SerialNumber 2.5.4.5	Entero positivo asignado unívocamentepor la AC-DIGILOGIX a cada certificado
Algoritmo de Firma	SignatureAlgorithm 2.5.8.3	sha256-RSA 1.2.840.113549.1.1.11
Issuer (Nombre distintivo del emisor)	commonName 2.5.4.3	AC-DIGILOGIX
	serialNumber 2.5.4.5	CUIT 30714128716
	organizationName 2.5.4.10	DIGILOGIX S.A.
	stateOrProvinceName 2.5.4.8	Ciudad Autónoma deBuenos Aires
	countryName 2.5.4.6	AR
Validez (desde, hasta)	notBefore	(Válido desde) <fecha, hora, minutos y segundos deemisión> Fecha y hora en que el período de vigencia delcertificado comienza
	notAfter	(Válido hasta) <fecha, hora, minutos y segundos deemisión + 2 años> Fecha y hora en que elperiodo de vigencia del certificado termina
Subject (Nombre distintivo del suscriptor)	commonName 2.5.4.3	Nombres y Apellidos
	serialNumber 2.5.4.5	CUIT o CUIL y sunúmero
	countryName 2.5.4.6	Código de País deacuerdo a ISO3166
SubjectPublicKeyInfo (Clave pública del suscriptor)	Publickeyalgorithm	RSA 1.2.840.113549.1.1.1
	Publickeylength	2048 bits Longitud de la clavepública del suscriptor
	Public key	<Clave pública del suscriptor> Valor de la clave pública del suscriptor

Extensiones del certificado (Extensions)		
Restricciones básicas	Basic Constraints 2.5.29.19	Tipo de asunto = Entidad final pathLenghtConstraint = Null
Usos de clave	Key Usage 2.5.29.15	digitalSignature = 1 contentCommitment= 1 keyEncipherment = 1 dataEncipherment = 1 keyAgreement = 0 keyCertSign = 0 cRLSign = 0 encipherOnly = 0 decipherOnly = 0
Identificador de clave del Suscriptor	Subject Key Identifier 2.5.29.14	Contiene un hash de 20bytes del atributo clavepública del suscriptor
Puntos de Distribución de la Lista de Certificados Revocados	CRLDistributionPoints 2.5.29.31	[1] Punto de distribución CRL Dirección URL=http://www.digilogix.com.ar/ar/digilogixv3.crl [2] Punto de distribución CRL Dirección URL=http://backup.digilogix.com.ar/ar/digilogixv3.crl
Política de Certificación	CertificatePolicies 2.5.29.32	OID de la Política de Certificación de DIGILOGIX S.A OID=2.16.32.1.1.7 URL de la Política: https://www.digilogix.com.ar/documentos/cpsv3.pdf Texto de aviso=certificado emitido por un certificador licenciado en el marco de la Ley 25.506
Identificador de la Clavede la Autoridad Certificante	AuthorityKeyIdentifier 2.5.29.35	Contiene un hash de 20 bytes del atributo clave pública del DIGILOGIX AC que emitió el certificado.
Uso Extendido de Clave	Extended Key Usage 2.5.29.37	Autenticación del cliente (1.3.6.1.5.5.7.3.2) Correo seguro (1.3.6.1.5.5.7.3.4)
Nombres Alternativos del Suscriptor	SubjectAlternativeName 2.5.29.17	Dirección de mail del suscriptor verificada porcircuito seguro compatible con RFC822

Acceso Informaciónemisor	AuthorityInfoAccess 1.3.6.1.5.5.7.1.1	[1] Authority Info Access Access Method=On-line Certificate Status Protocol (1.3.6.1.5.5.7.48.1) Alternative Name: URL=http://ocspv3.digilogix.com.ar/ocsp [2] Authority Info Access Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2) Alternative Name: URL=http://www.digilogix.com.ar/ar/digilogixv3.crt
Declaraciones de certificados calificados	QCStatement 1.3.6.1.5.5.7.1.3	OID=2.16.32.1.10.1, cuando las claves seangeneradas por software. OID=2.16.32.1.10.2.1, cuando las claves seangeneradas en dispositivos que cuenten con certificación FIPS 140 (Versión 2) nivel 1. OID=2.16.32.1.10.2.2, cuando las claves sean generadas en dispositivos que cuenten con certificación FIPS 140 (Versión 2) nivel 2. OID=2.16.32.1.10.2.3, cuando las claves sean generadas en dispositivos que cuenten con certificación FIPS 140 (Versión 2) nivel 3

b) Perfil del certificado de la persona jurídica

Campos Atributos Extensiones	**Valor/OID**	**Contenido**
Versión	Version	2 Corresponde a versión 3
Número de serie	SerialNumber 2.5.4.5	Entero positivo asignadounívocamente por la AC-DIGILOGIX a cada certificado
Algoritmo de Firma	SignatureAlgoritm 2.5.8.3	sha256-RSA 1.2.840.113549.1.1.11
Issuer (Nombre distintivo del emisor)	commonName 2.5.4.3	AC-DIGILOGIX
	serialNumber 2.5.4.5	30714128716

	organizationName 2.5.4.10	DIGILOGIX S.A.
	stateOrProvinceName 2.5.4.8	Ciudad Autónoma de BuenosAires
	countryName 2.5.4.6	AR
Validez (desde,hasta)	notBefore	(Válido desde) <fecha,hora, minutos ysegundos de emisión> Fecha y hora en que el período de vigencia del certificadocomienza
	notAfter	(Válido hasta) <fecha,hora, minutos y segundos de emisión +2 años> Fecha y hora en que el periodo de vigencia del certificado termina
Subject (Nombre distintivo del suscriptor)	commonName 2.5.4.3	Denominación de la PersonaJurídica
	serialNumber 2.5.4.5	CUIT de la Persona Jurídica
	OrganizationName 2.5.4.10	Nombre de la organización
	organizationalUnitName 2.5.4.11	Nombre de la suborganización
	countryName 2.5.4.6	AR
SubjectPublicKeyInfo (Clave pública del suscriptor)	publickeyalgorithm	RSA 1.2.840.113549.1.1.1
	Publickeylength	2048 bits Longitud de la clave pública del suscriptor
	Public key	< Clave pública del suscriptor> Valor de la clave pública del suscriptor
Extensiones del certificado (Extensions)		
Restricciones básicas	Basic Constraints 2.5.29.19	Tipo de asunto = Entidad final pathLenghtConstraint = Null
Usos de clave	Key Usage 2.5.29.15	digitalSignature = 1 contentCommitment= 1 keyEncipherment = 1 dataEncipherment = 1 keyAgreement = 0 keyCertSign = 0 cRLSign = 0

		encipherOnly = 0 decipherOnly = 0
Identificador de clavedel Suscriptor	Subject Key Identifier 2.5.29.14	Contiene un hash de 20 bytes del atributo clave pública delsuscriptor
Puntos de Distribución de la Lista de Certificados Revocados	CRLDistributionPoints 2.5.29.31	[1] Punto de distribución CRL Dirección URL=http://www.digilogix.com.ar/ar/digilogixv3.crl [2] Punto de distribución CRL Dirección URL=http://backup.digilogix.com.ar/ar/digilogixv3.crl
Política de Certificación	CertificatePolicies 2.5.29.32	OID de la Política de Certificación de DIGILOGIX S.A OID=2.16.32.1.1.7 URL de la Política: https://www.digilogix.com.ar/documentos/cpsv3.pdf Texto de aviso=certificado emitido por un certificador licenciado en el marco de la Ley 25.506
Identificador de la Clave de la Autoridad Certificante	AuthorityKeyIdentifier 2.5.29.35	Contiene un hash de 20 bytes del atributo clave pública del DIGILOGIX AC que emitió el certificado.
Uso Extendido de Clave	Extended Key Usage 2.5.29.37	Autenticación del cliente (1.3.6.1.5.5.7.3.2) Correo seguro (1.3.6.1.5.5.7.3.4)
SubjectAlternativeName (Nombres Alternativos del Suscriptor)	commonName 2.5.4.3	Nombres y Apellidos
	serialNumber 2.5.4.5	CUIT o CUIL y número del mismo
	title 2.5.4.12	Cargo o título del suscriptor dentro de la organización, debe corresponder con la certificación aportada en el proceso deautenticación
Acceso Información Emisor	AuthorityInfoAccess 1.3.6.1.5.5.7.1.1	[1] Authority Info Access Access Method=On-line Certificate Status Protocol (1.3.6.1.5.5.7.48.1) Alternative Name: URL=http://ocspv3.digilogix.com.ar/ocsp [2] Authority Info Access Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2) Alternative Name: URL=http://www.digilogix.com.ar/ar/digilogixv3.crt

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

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

- **Perfil del certificado de aplicaciones**

Certificado x.509 v3 Atributos Extensiones	**Valor/OID**	**Contenido**
Versión	Version	2 Corresponde a versión 3
Número de serie	SerialNumber 2.5.4.5	Entero positivo asignado unívocamente por la AC DIGILOGIX a cada certificado
Algoritmo de Firma	signatureAlgoritm 2.5.8.3	sha256RSA 1.2.840.113549.1.1.11
Issuer (Nombre distintivo del emisor)	commonName 2.5.4.3	AC-DIGILOGIX
	serialNumber 2.5.4.5	CUIT 30714128716
	organizationName 2.5.4.10	DIGILOGIX S.A.
	stateOrProvinceName 2.5.4.8	Ciudad Autónoma de Buenos Aires
	countryName 2.5.4.6	AR
Validez (desde, hasta)	notBefore	(Válido desde) <fecha, hora, minutos ysegundos de emisión> Fecha y hora en que el período devigencia

		del certificado comienza
	notAfter	(Válido hasta) <fecha,hora, minutos y segundos de emisión + 2 años> Fecha y hora en que el periodo devigencia del certificado termina
Subject DN (Nombre distintivo del suscriptor)	commonName 2.5.4.3	CN=Denominación de la Aplicación
	organizationName 2.5.4.10	O=Nombre de la Persona Jurídica Pública o Privada responsable de laaplicación
	organizationalUnitName 2.5.4.11	OU=Unidad Operativa relacionada con la aplicación
	serialNumber 2.5.4.5	serialNumber=CUIT y su número
	countryName 2.5.4.6	C=AR
SubjectPublicKeyInfo (Clave pública del suscriptor)	publickeyalgorithm	RSA 1.2.840.113549.1.1.1
	Publickeylength	2048 bits Longitud de la clave pública delsuscriptor
	Public key	<Clave pública del suscriptor> Valor de la clave pública del suscriptor
Extensiones del certificado (Extensions)		
Restricciones básicas	Basic Constraints 2.5.29.19	Tipo de asunto = Entidad final pathLenghtConstraint = Null
Usos de clave	Key Usage 2.5.29.15	digitalSignature = 1 contentCommitment = 1 keyEncipherment = 1 dataEncipherment = 1 keyAgreement = 0 keyCertSign = 0 cRLSign = 0 encipherOnly = 0 decipherOnly = 0
Identificador de clavedel Suscriptor	Subject Key Identifier 2.5.29.14	Contiene un hash de 20 bytes del atributo clave pública del suscriptor
Puntos de Distribución de la Lista de Certificados Revocados	CRLDistributionPoints 2.5.29.31	[1] Punto de distribución CRL Dirección URL=http://www.digilogix.com.ar/ar/digilogixv3.crl [2] Punto de distribución CRL Dirección URL=http://backup.digilogix.com.ar/ar/digilogixv3.crl

Política de Certificación	CertificatePolicies 2.5.29.32	OID de la Política de Certificación de DIGILOGIX S.A OID=2.16.32.1.1.7 URL de la Política: https://www.digilogix.com.ar/documentos/cpsv3.pdf Texto de aviso=certificado emitido por un certificador licenciado en el marco de la Ley 25.506
Identificador de la Clave de la Autoridad Certificante	AuthorityKeyIdentifier 2.5.29.35	Contiene un hash de 20 bytes del atributo clave pública del DIGILOGIXAC que emitió el certificado.
Uso Extendido deClave	Extended Key Usage 2.5.29.37	Autenticación del cliente(1.3.6.1.5.5.7.3.2)
Acceso Información emisor	AuthorityInfoAccess 1.3.6.1.5.5.7.1.1	[1] Authority Info Access Access Method=On-line Certificate Status Protocol (1.3.6.1.5.5.7.48.1) Alternative Name: URL=http://ocspv3.digilogix.com.ar/ocsp [2] Authority Info Access Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2) Alternative Name: URL=http://www.digilogix.com.ar/ar/digilogixv3.crt
Declaraciones de certificados calificados	QCStatement 1.3.6.1.5.5.7.1.3	OID=2.16.32.1.10.1, cuando las claves sean generadas por software. OID=2.16.32.1.10.2.1, cuando las claves sean generadas en dispositivos que cuenten con certificación FIPS 140 (Versión 2) nivel 1. OID=2.16.32.1.10.2.2, cuando lasclaves sean generadas en dispositivos que cuenten con certificación FIPS 140 (Versión 2) nivel 2. OID=2.16.32.1.10.2.3, cuando lasclaves sean generadas en dispositivos que cuenten con certificación FIPS 140 (Versión 2) nivel 3.

- **Perfil del certificado de Autoridad de Sello de Tiempo**

Campos Atributos Extensiones	Nombre del campo y OID	Contenido
Versión	Version	2 Corresponde a versión 3
Número de serie	SerialNumber 2.5.4.5	Entero positivo asignadounívocamente por la AC DIGILOGIX a cada certificado
Algoritmo de Firma	signatureAlgoritm	sha256RSA 1.2.840.113549.1.1.11
Issuer (Nombre distintivo del emisor)	commonName 2.5.4.3	AC-DIGILOGIX
	serialNumber 2.5.4.5	30714128716
	organizationName 2.5.4.10	DIGILOGIX S.A.
	stateOrProvinceName 2.5.4.8	Ciudad Autónoma de Buenos Aires
	countryName 2.5.4.6	AR
Validez (desde, hasta)	notBefore	(Válido desde) <fecha, hora, minutos ysegundos de emisión> Fecha y hora en que el período devigencia del certificado comienza
	notAfter	(Válido hasta) <fecha, hora, minutos y segundos de emisión + 2años> Fecha y hora en que el periodo devigencia del certificado termina
Subject DN (Nombre distintivo del suscriptor)	commonName 2.5.4.3	CN=Denominación del servicio de emisión de sello de tiempo
	organizationName 2.5.4.10	O=Unidad Operativa relacionada con el suscriptor
	organizationalUnitName 2.5.4.11	OU=Nombre de la Persona Jurídica Pública o Privada responsable del servicio
	serialNumber 2.5.4.5	serialNumber=CUIT y su número
	countryName 2.5.4.6	C=AR
SubjectPublicKeyInfo	publickeyalgorithm	RSA 1.2.840.113549.1.1.1
	Publickeylength	2048 bits Longitud de la clave pública
	Public key	<Clave pública delsuscriptor>

		Valor de la clave pública
Extensions (Extensiones del certificado)		
Restricciones básicas	Basic Constraints 2.5.29.19	Tipo de asunto = Entidad final pathLenghtConstraint = Null
Usos de clave	Key Usage 2.5.29.15	digitalSignature = 1 contentCommitment = 1 keyEncipherment =1 dataEncipherment = 1 keyAgreement = 0 keyCertSign = 0 cRLSign = 0 encipherOnly = 0 decipherOnly = 0
Identificador de clavedel Suscriptor	Subject Key Identifier 2.5.29.14	Contiene un hash de 20 bytes del atributo clave pública del suscriptor
Puntos de Distribución de la Lista de Certificados Revocados	CRLDistributionPoints 2.5.29.31	[1] Punto de distribución CRL Dirección URL=http://www.digilogix.com.ar/ar/digilogix v3.crl [2] Punto de distribución CRL Dirección URL=http://backup.digilogix.com.ar/ar/digilo gixv3.crl
Política de Certificación	CertificatePolicies 2.5.29.32	OID de la Política de Certificación de DIGILOGIX S.A OID=2.16.32.1.1.7 URL de la Política: https://www.digilogix.com.ar/documentos/cp sv3.pdf Texto de aviso=certificado emitido por un certificador licenciado en el marco de la Ley 25.506
Identificador de la Clave de la Autoridad Certificante	AuthorityKeyIdentifier 2.5.29.35	Contiene un hash de 20 bytes del atributo clave pública del DIGILOGIXAC que emitió el certificado.
Uso Extendido deClave	Extended Key Usage 2.5.29.37	Autenticación del cliente(1.3.6.1.5.5.7.3.2) Certificación digital de fecha y hora (1.3.6.1.5.5.7.3.8)
Acceso Información emisor	AuthorityInfoAccess 1.3.6.1.5.5.7.1.1	[1] Authority Info Access Access Method=On-line Certificate Status Protocol (1.3.6.1.5.5.7.48.1) Alternative Name: URL=http://ocspv3.digilogix.com.ar/ocsp [2] Authority Info Access Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2) Alternative Name:

		URL=http://www.digilogix.com.ar/ar/digilogix v3.crt
Declaraciones de certificados calificados	QCStatement 1.3.6.1.5.5.7.1.3	OID=2.16.32.1.10.2.3, clave generadaen dispositivos que cuenten con certificación FIPS 140 (Versión 2) nivel 3.

- **Perfil del certificado de Autoridad de Sello de Competencia**

Certificado x.509 v3 Atributos Extensiones	Nombre del campo y OID	Contenido
Versión	Version	2 Corresponde a versión 3
Número de serie	SerialNumber 2.5.4.5	Entero positivo asignadounívocamente por la AC DIGILOGIX a cada certificado
Algoritmo de Firma	signatureAlgoritm	sha256RSA 1.2.840.113549.1.1.11
Issuer (Nombre distintivo del emisor)	commonName 2.5.4.3	AC-DIGILOGIX
	serialNumber 2.5.4.5	30714128716
	organizationName 2.5.4.10	DIGILOGIX S.A.
	stateOrProvinceName 2.5.4.8	Ciudad Autónoma de Buenos Aires
	countryName 2.5.4.6	AR
Validez (desde, hasta)	notBefore	(Válido desde) <fecha, hora, minutos ysegundos de emisión> Fecha y hora en que el período de vigencia del certificado comienza
	notAfter	(Válido hasta) <fecha,hora, minutos y segundos de emisión + 2años> Fecha y hora en que el periodo de vigencia del certificado termina
Subject DN (Nombre distintivo del suscriptor)	commonName 2.5.4.3	Denominación del servicio de emisión de sello de competencia
	organizationName 2.5.4.10	Nombre de la Persona Jurídica Pública o Privada responsable de la aplicación
	organizationalUnitName 2.5.4.11	Unidad Operativa relacionada con la aplicación

	serialNumber 2.5.4.5	CUIT y su número
	countryName 2.5.4.6	AR
SubjectPublicKeyInfo (Clave pública del suscriptor)	publickeyalgorithm	RSA 1.2.840.113549.1.1.1
	Publickeylength	2048 bits Longitud de la clave pública del suscriptor
	Public key	<Clave pública delsuscriptor> Valor de la clave pública del suscriptor
Extensions (Extensiones del certificado)		
Basic Constraints (Restricciones básicas)	2.5.29.19	Tipo de asunto = Entidad final pathLenghtConstraint = Null
Key Usage (Usos de clave)	2.5.29.15	digitalSignature = 1 contentCommitment = 1 keyEncipherment = 1 dataEncipherment = 0 keyAgreement = 0 keyCertSign = 0 cRLSign = 0 encipherOnly = 0 decipherOnly = 0
Subject Key Identifier (Identificador de clavedel Suscriptor)	2.5.29.14	Contiene un hash de 20 bytes del atributo clave pública del suscriptor
Puntos de Distribución de la Lista de Certificados Revocados	CRLDistributionPoints 2.5.29.31	[1] Punto de distribución CRL Dirección URL=http://www.digilogix.com.ar/ar/digilogixv3.crl [2] Punto de distribución CRL Dirección URL=http://backup.digilogix.com.ar/ar/digilogixv3.crl
Política de Certificación	CertificatePolicies 2.5.29.32	OID de la Política de Certificación de DIGILOGIX S.A OID=2.16.32.1.1.7 URL de la Política: https://www.digilogix.com.ar/documentos/cpsv3.pdf Texto de aviso=certificado emitido por un certificador licenciado en el marco de la Ley 25.506
Identificador de la Clave de la Autoridad Certificante	AuthorityKeyIdentifier 2.5.29.35	Contiene un hash de 20 bytes del atributo clave pública del DIGILOGIXAC que emitió el certificado.
Uso Extendido deClave	Extended Key Usage	Autenticación del cliente

	2.5.29.37	(1.3.6.1.5.5.7.3.2)
Acceso Información emisor	AuthorityInfoAccess 1.3.6.1.5.5.7.1.1	[1] Authority Info Access Access Method=On-line Certificate Status Protocol (1.3.6.1.5.5.7.48.1) Alternative Name: URL=http://ocspv3.digilogix.com.ar/ocsp [2] Authority Info Access Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2) Alternative Name: URL=http://www.digilogix.com.ar/ar/digilogixv3.crt
Declaraciones de certificados calificados	QCStatement 1.3.6.1.5.5.7.1.3	OID=2.16.32.1.10.2.3, clave generada en dispositivos que cuenten con certificación FIPS 140(Versión 2) nivel 3

7.2.- Perfil de la Lista de Certificados Revocados

Campos Atributos Extensiones	Valor/OID	Observaciones
Versión	Version	1 Corresponde a versión 2
Algoritmo de Firma	signatureAlgoritm	sha256RSA 1.2.840.113549.1.1.11
Issuer (Nombre distintivo del emisor)	commonName 2.5.4.3	AC-DIGILOGIX
	serialNumber 2.5.4.5	CUIT 30714128716
	organizationName 2.5.4.10	DIGILOGIX S.A.
	stateOrProvinceName 2.5.4.8	Ciudad Autónoma de Buenos Aires
	countryName 2.5.4.6	AR
Validity (Not before, not after) Validez (desde, hasta)		
Día y hora de vigencia	thisUpdate	<fecha y hora UTC> yyyy/mm/ddhh:mm:sshuso-horario Fecha y hora efectivas de emisión, a partir de la cual entre en vigencia
Próxima Actualización	nextUpdate	<fecha y hora UTC> yyyy/mm/ddhh:mm:ss huso-horario Fecha y hora de emisión de lapróxima

		Lista de Certificados Revocados
Identificador de la Clave de la Autoridad Certificante	AuthorityKeyIdentifier 2.5.29.35	Contiene un hash de 20 bytes del atributo clave pública del DIGILOGIX AC que emitió la Lista de Certificados Revocados.
Número de CRL	CRL Number 2.5.29.20	Número incremental que identifica la CRL emitida
Punto de distribución de emisión	issuingDistributionPoint 2.5.29.28	Nombre de punto de distribución: Nombre completo: Dirección URL=http://www.digilogix.com.ar/ar/digilogixv3.crl Dirección URL=http://backup.digilogix.com.ar/ar/digilogixv3.crl Solo contiene Certificados de usuario=No Solo contiene Certificados de la CA=No Lista de revocación de certificados (CRL) indirecta=No
CRL más reciente	freshestCRL 2.5.29.46	[1]Lista de revocación de certificados (CRL) más actualizada Nombre del punto de distribución: Nombre completo: Dirección URL=http://www.digilogix.com.ar/ar/digilogixv3+.crl Dirección URL=http://backup.digilogix.com.ar/ar/digilogixv3+.crl
Indicador Delta CRL	Delta CRL Indicator 2.5.29.27	Número que se incrementa cada vez que se emite una Delta CRL
Certificados Revocados (RevokedCertificates)		
Fecha de Revocación	<fecha y hora UTC> yyyy/mm/ddhh:mm:sshuso-horario	Fecha y hora en que se revocó el certificado
Número de Serie del Certificado revocado	Serial Number hasta 20 octetos 2.5.4.5	Número de Serie del Certificado revocado
Motivo de laRevocación	ReasonCode 2.5.29.21	Motivo de la Revocación
Versión de CA	V0.0	Versión de CA

7.3.- Perfil de la consulta en línea del estado del certificado

Perfil del Certificado del Servicio de Consulta OCSP

Campos Atributos Extensiones	Valor/OID	Contenido
Versión	Version	2 Corresponde a versión 3
Número de serie	SerialNumber 2.5.4.5	Entero positivo asignadounívocamente por la AC DIGILOGIX a cada certificado
Algoritmo de Firma	signatureAlgoritm	sha256RSA 1.2.840.113549.1.1.11
Issuer (Nombre distintivo del emisor)		
Issuer (Nombre distintivo del emisor)	commonName 2.5.4.3	AC-DIGILOGIX
	serialNumber 2.5.4.5	CUIT 30714128716
	organizationName 2.5.4.10	DIGILOGIX S.A.
	stateOrProvinceName 2.5.4.8	Ciudad Autónoma de Buenos Aires
	countryName 2.5.4.6	AR
Validez (desde, hasta)	notBefore	<fecha, hora, minutos ysegundos de emisión> Fecha y hora en que el período devigencia del certificado comienza
	notAfter	<fecha,hora, minutos y segundos de emisión + 2años> Fecha y hora en que el periodo devigencia del certificado termina
Nombre distintivo del suscriptor (Subject)	commonName 2.5.4.3	OCSP-DIGILOGIX
	serialNumber 2.5.4.5	CUIT 30714128716
	organizationName 2.5.4.10	DIGILOGIX S.A.
	stateOrProvinceName 2.5.4.8	Ciudad Autónoma de Buenos Aires
	countryName 2.5.4.6	AR
SubjectPublicKeyInfo (Clave pública del suscriptor)	publickeyalgorithm	Tipo de algoritmo de clave públicautilizado
	Publickeylength	Longitud de la clave pública delsuscriptor
	Public key	Valor de la clave pública del suscriptor
Extensions (Extensiones del certificado)		

Restricciones básicas	Basic Constraints 2.5.29.19	Tipo de asunto = Entidad final pathLenghtConstraint = Null
Usos de clave	Key Usage 2.5.29.15	digitalSignature = 1 contentCommitment= 1 keyEncipherment = 0 dataEncipherment = 0 keyAgreement = 0 keyCertSign = 0 cRLSign = 0 encipherOnly = 0 decipherOnly = 0
Identificador de clavedel Suscriptor	Subject Key Identifier 2.5.29.14	Contiene un hash de 20 bytes del atributo clave pública del suscriptor
Puntos de Distribución de la Lista de Certificados Revocados	CRLDistributionPoints 2.5.29.31	[1] Punto de distribución CRL Dirección URL=http://www.digilogix.com.ar/ar/digilogixv3.crl [2] Punto de distribución CRL Dirección URL=http://backup.digilogix.com.ar/ar/digilogixv3.crl
Política de Certificación	CertificatePolicies 2.5.29.32	OID de la Política de Certificación de DIGILOGIX S.A OID=2.16.32.1.1.7 URL de la Política: https://www.digilogix.com.ar/documentos/cpsv3.pdf Texto de aviso=certificado emitido por un certificador licenciado en el marco de la Ley 25.506
Identificador de la Clave de la Autoridad Certificante	AuthorityKeyIdentifier 2.5.29.35	Contiene un hash de 20 bytes del atributo clave pública del DIGILOGIXAC que emitió el certificado.
Uso Extendido deClave	Extended Key Usage 2.5.29.37	OCSPSigning (1.3.6.1.5.5.7.3.9) Corresponde a las respuestas delservicio OCSP
Nombres Alternativos del Suscriptor	SubjectAlternativeName 2.5.29.17	DNS Name=http://ocspv3.digilogix.com.ar/ocsp
Acceso Información emisor	AuthorityInfoAccess 1.3.6.1.5.5.7.1.1	[1] Authority Info Access Access Method=On-line Certificate Status Protocol (1.3.6.1.5.5.7.48.1) Alternative Name: URL=http://ocspv3.digilogix.com.ar/ocsp [2] Authority Info Access Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2) Alternative Name: URL=http://www.digilogix.com.ar/ar/digilogixv3.crt

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

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 un certificado digital emitido por la

AC – DIGILOGIX para tal fin 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. – AUDITORÍA 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 SECRETARIA DE INNOVACION, CIENCIA Y TECNOLOGIA, en cumplimiento con la Resolución N° 946/21.

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

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

Los informes resultantes de las auditorías son elevados a la SECRETARIA DE INNOVACION, CIENCIA Y TECNOLOGIA.

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

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

El certificador cumple las exigencias reglamentarias impuestas por:

a) Los artículos 33 y 34 de la Ley Nº 25.506 de Firma Digital, respecto al sistema de auditoría y el artículo 21, inciso k) de la misma ley, relativo a la publicación de informes de auditoría.
b) Los art. 6, 7 y 8 del Decreto Nº 182/19, relativos al sistema de auditoría.

9. – ASPECTOS LEGALES Y ADMINISTRATIVOS

9.1. – Aranceles

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

distintos tipos de certificados.

9.2. - Responsabilidad Financiera

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

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 **AC - DIGILOGIX** o la Autoridad de Registro durante el ciclo de vida del certificado.

Digilogix SA, en su carácter de certificador, garantiza la confidencialidad frente a terceros de su clave privada, la que, al ser el punto de máxima confianza, será generada y custodiada conforme a lo que se especifique en la presente Política. Asimismo, se considera confidencial cualquier información:

- Resguardada en servidores o bases de datos y vinculada al proceso de gestión del ciclo de vida de los certificados digitales emitidos por **AC - DIGILOGIX**.

- Almacenada en cualquier soporte, incluyendo aquella que se trasmita verbalmente, vinculada a procedimientos de certificación, excepto aquella declarada como no confidencial en forma expresa.
- Relacionada con los Planes de Continuidad de operaciones, controles, procedimientos de seguridad y registros de auditoría pertenecientes a **AC - DIGILOGIX**.

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

9.3.2. - Información no confidencial

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

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

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

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

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

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

9.3.3. – Responsabilidades de los roles involucrados

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

Toda divulgación de información referida a los datos de identificación del suscriptor o a cualquier otra información generada o recibida durante el ciclo de vida del certificado sólo

podrá efectuarse previa autorización escrita del suscriptor del certificado.

No será necesario el consentimiento cuando:

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

9.4. – Privacidad

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

9.5 - Derechos de Propiedad Intelectual

El derecho de autor de los sistemas y aplicaciones informáticas desarrollados por el Certificador para la implementación de su AC, como así toda la documentación relacionada, pertenece a **DIGILOGIX S.A.**

Consecuentemente, dichos documentos no pueden ser reproducidos, copiados ni utilizados de ninguna manera, total o parcial, sin previo y formal consentimiento de **DIGILOGIX S.A.**, de acuerdo a la legislación vigente.

9.6. – Responsabilidades y garantías

Las responsabilidades y garantías para **AC - DIGILOGIX**, sus Autoridades de Registro, los

suscriptores, los terceros usuarios y otras entidades participantes, se rigen por lo establecido por la Ley N° 25.506, su Decreto Reglamentario Nº 182/19, la Resolución N° 946/21 y toda otra normativa complementaria.

Asimismo, las partes contratantes se rigen por el Acuerdo con Suscriptores, como contrato específico que regula la relación entre el suscriptor y el Certificador Licenciado DIGILOGIX S.A.

9.7. – Deslinde de responsabilidad

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

9.8. – Limitaciones a la responsabilidad frente a terceros

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

9.9. – Compensaciones por daños y perjuicios

No aplicable.

9.10. – Condiciones de vigencia

La presente Política Única de Certificación 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 la Política, 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

Toda modificación a la Política Única de Certificación es aprobada previamente por el Ente Licenciante conforme a lo establecido por la Ley N° 25.506, art. 21, inciso q) y por la Resolución N° 946/21 y sus anexos respectivos.

Todo cambio en la Política Única de Certificación es comunicado al suscriptor.

La presente Política Única de Certificación será revisada y actualizada periódicamente por el **– DIGILOGIX S.A.** y sus nuevas versiones se pondrán en vigencia, previa aprobación del Ente Licenciante.

9.12.2 – Mecanismo y plazo de publicación y notificación

Una copia de la versión vigente de la presente Política Única de Certificación se encuentra disponible en forma pública y accesible a través de Internet en el sitio web https://www.digilogix.com.ar/documentos

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

9.12.3. – Condiciones de modificación del OID

No aplicable.

9.13. - Procedimientos de resolución de conflictos

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

La presente Política Única de Certificación se encuentra en un todo subordinada a las prescripciones de la Ley N° 25.506 y su reglamentación.

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

Una vez recibido el reclamo en las oficinas de **DIGILOGIX S.A.** este citará al reclamante a una audiencia y labrará un acta que deje expresa constancia de los hechos que motivan el reclamo y de todas y cada uno de los antecedentes que le sirvan de causa. Dará traslado del acta, mediante notificación fehaciente, a las partes involucradas, Autoridad de Registro y/o Suscriptor y/o Tercero Usuario. Estas partes dispondrán un plazo de DIEZ (10) días corridos para ofrecer y producir prueba que haga a su defensa y aleguen sobre el mérito de la misma. Finalmente, **DIGILOGIX SA** resolverá en un plazo de DIEZ (10) días corridos conforme a los criterios de máxima razonabilidad, equidad y pleno ajuste al bloque de legalidad vigente y aplicable.

Las partes involucradas en el conflicto podrán recurrir ante la Autoridad de Aplicación, previo agotamiento del procedimiento administrativo recién descripto y sin perjuicio de su derecho de acudir directamente a la vía judicial correspondiente.

En ningún caso la Política Única de Certificación del certificador prevalecerá sobre lo dispuesto por la normativa legal vigente de firma digital.

9.14. - Legislación aplicable

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

9.15. – Conformidad con normas aplicables

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

9.16. – Cláusulas adicionales

No se establecen cláusulas adicionales.

9.17. – Otras cuestiones generales

Versión y Modificación	Fecha de emisión	Revisado por	Descripción
Versión 1.0	22/05/2015	Directorio DIGILOGIX	Aprobación para presentación
Versión 2.0	09/11/2022	Directorio DIGILOGIX	Renovación de licencia
Versión 3.0	Desde la publicación en B.O.	Directorio DIGILOGIX	Renovación de certificado

República Argentina - Poder Ejecutivo Nacional
AÑO DE LA DEFENSA DE LA VIDA, LA LIBERTAD Y LA PROPIEDAD

Hoja Adicional de Firmas
Informe gráfico

Número: IF-2024-44491979-APN-DNFDEIT#JGM

CIUDAD DE BUENOS AIRES
Martes 30 de Abril de 2024

Referencia: Anexo I POLITICA UNICA DE CERTIFICACION V3

El documento fue importado por el sistema GEDO con un total de 87 pagina/s.

Digitally signed by GESTION DOCUMENTAL ELECTRONICA - GDE
Date: 2024.04.30 17:50:19 -03:00

Enrique Manuel CARRIZO
Director
Dirección Nacional de Firma Digital e Infraestructura Tecnológica
Jefatura de Gabinete de Ministros

Digitally signed by GESTION DOCUMENTAL ELECTRONICA - GDE
Date: 2024.04.30 17:50:21 -03:00