ANEXO I

FORMULARIO DE ADHESIÓN A LA POLÍTICA ÚNICA DE CERTIFICACIÓN

CERTIFICADOR LICENCIADO
DIGILOGIX S.A.

Versión 1.0

INTRODUCCIÓN.

El presente “Formulario de Adhesión a la Política Única de Certificación” fue aprobado por el artículo 1º de la Decisión Administrativa Nº 927 del 30 de octubre de 2014 que, como Anexo I forma parte de la cita norma.

Se indican en el mismo aquella información particular de su actividad que está señalada como variable en la Política Única de Certificación, aprobada por el Anexo III de la Decisión Administrativa Nº 927/14.

La presentación de este formulario por parte de **DIGILOGIX S.A.** implica la aceptación de la Política Única de Certificación como la aplicable para ejercer sus funciones como parte de la Infraestructura de Firma Digital de la REPÚBLICA ARGENTINA aprobada por Ley Nº 25.506.

Nombre e Identificación de la Política Única de Certificación.

Ref: 1.2. – Nombre e Identificación del Documento.

a) Nombre: Política Única de Certificación de **DIGILOGIX S.A.**
b) Versión: 1.0
c) Fecha de aplicación: a partir de la fecha del otorgamiento de la licencia por el Ente Licenciante.
d) Lugar o sitio de publicación: se publica en el sitio web de la **AC - DIGILOGIX** http://www.digilogix.com.ar/documentos/
e) OID de la Política de Certificación:

Datos del Certificador.

Ref: 1.3.1. – Certificador.

DIGILOGIX S.A.

Domicilio: Calle: Rivadavia 789 Piso 4º Código Postal: C1002AAF

Ciudad Autónoma de Buenos Aires.

Correo electrónico: info@digilogix.com.ar

Teléfono: +54 11 5917-5890

Datos de las Autoridades de Registro.

Ref: 1.3.2. - Autoridad de Registro.

Las Autoridades de Registro del Certificador que han sido habilitadas para operar, incluyendo su domicilio, datos de contacto y si operan bajo la modalidad de Autoridades de Registro Móviles, se encuentran disponibles en su sitio web: http://www.digilogix.com.ar/ar

Comunidad de Suscriptores y Terceros Usuarios.

Ref: 1.3.3. - Suscriptores de certificados y 1.3.4. – Terceros Usuarios.

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

- **a)** Las personas físicas 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 físicas 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 físicas y/o jurídicas vinculadas a cualquier actividad, entre otras, relacionada con funciones de tramitación y administrativas aduaneras.
- **d)** Certificados para proveedores de servicios en relación a la firma digital, conforme a lo dispuesto en el artículo 10 de la Decisión Administrativa Nº 927 del 30 de octubre de 2014.

Son Terceros Usuarios de los certificados emitidos bajo la presente Política Única de Certificación, toda persona física o jurídica que recibe un documento firmado digitalmente y que genera una consulta para verificar la validez del certificado digital correspondiente, de acuerdo al Anexo I del Decreto N° 2628 del 19 de diciembre de 2002. En el caso de los certificados de sitio seguro, serán Terceros Usuarios quienes verifiquen el certificado del servidor.

Responsable del Documento.

Ref: 1.5.1. – Responsable del documento.

Será responsable de la presente Política Única del Certificador quien ejerza las funciones de Responsable de la **AC – DIGILOGIX:**
Correo electrónico: info@digilogix.com.ar
Teléfono: +54 11 5917-5890

Contacto.

Ref: 1.5.2. – Contacto.

La presente Política Única de Certificación es administrada por la Máxima autoridad del Certificador Licenciado:
Correo electrónico: info@digilogix.com.ar
Teléfono: +54 11 5917-5890

Procedimiento de aprobación de la Política Única de Certificación.

Ref: 1.5.3. – Procedimiento de aprobación de la Política Única de Certificación.

La Política Única de Certificación y el Formulario de Adhesión del Anexo I han sido presentados ante el ente licenciante durante el proceso de licenciamiento aprobado por Disposición S.S.T.G. Nº

Repositorios.

Ref: 2.1. – Repositorios.

El servicio de repositorio de información y la publicación de la Lista de Certificados Revocados son administrados en forma directa por el Certificador.

Publicación de información del certificador.

Ref: 2.2. - Publicación de información del certificador.

Adicionalmente a lo indicado, el Certificador mantiene en el mismo repositorio en línea de acceso público:

a) Las Política de Certificación anteriores

b) Información relevante de los informes de la última auditoría dispuesta por la Autoridad de Aplicación.

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 del Certificador.

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

El Certificador está obligado a brindar el servicio de repositorio en cumplimiento de lo dispuesto en el artículo 21 de la Ley N° 25.506, el Decreto N° 2628/02, y en la presente Política Única de Certificación.

- Obligaciones establecidas en el artículo 21 inciso k) de la Ley N° 25.506:

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

- Obligaciones establecidas en el artículo 34 incisos g), h) y m) del Decreto N° 2628/02:

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

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

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

Controles de acceso a la información.

Ref: 2.4. - Controles de acceso a la información.

No se agrega información.

Nombres Distintivos.

Ref: 3.1.2. - Necesidad de Nombres Distintivos.

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

a) “*commonName”* (OID 2.5.4.3: Nombre común): DEBE corresponder al nombre de la aplicación, servicio o de la unidad operativa responsable del servicio.

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

c) “*organizationName*” (OID 2.5.4.10: Nombre de la organización): DEBE estar presente y DEBE coincidir con el nombre de la Persona Jurídica Pública o Privada responsable del servicio o aplicación.

d) “*serialNumber*” (OID 2.5.4.5: Nro. de serie): DEBE estar presente y DEBE contener 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): DEBE estar presente y DEBE representar el país de emisión de los certificados, codificado según el estándar [ISO3166] de DOS (2) caracteres.

Para los certificados de Personas Físicas:

e) “*commonName*” (OID 2.5.4.3: Nombre común): DEBE estar presente y DEBE corresponderse con el nombre que figura en el Documento de Identidad del suscriptor, acorde a lo establecido en el punto 3.2.3.

f) “*serialNumber*” (OID 2.5.4.5: Nro. de serie): DEBE estar presente y DEBE contener 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:

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

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

- “*countryName*” (OID 2.5.4.6: Código de país): DEBE estar presente y DEBE representar 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:

a) “commonName” (OID 2.5.4.3: Nombre común): DEBE coincidir 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).

b) “organizationalUnitName” (OID 2.5.4.11: Nombre de la suborganización): PUEDE contener las unidades operativas relacionadas con el suscriptor, pudiendo utilizarse varias instancias de este atributo de ser necesario.

c) “organizationName” (OID 2.5.4.10: Nombre de la organización): para certificados de aplicaciones, DEBE coincidir con la denominación de la Persona Jurídica Pública o Privada.

d) “serialNumber” (OID 2.5.4.5: Nro de serie): DEBE estar presente y DEBE contener 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] DEBE estar codificado según el estándar [ISO3166] de 2 caracteres.

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

Para los certificados de sitio seguro:

g) “*commonName”* (OID 2.5.4.3: Nombre común): DEBE contener la denominación del sitio web de Internet que se busca proteger.

h) "*organizationalUnitName*" (OID 2.5.4.11: Nombre de la Suborganización): DEBE contener a las unidades operativas de las que depende el sitio web, de corresponder, pudiendo utilizarse varias instancias de este atributo de ser necesario.

i) "*organizationName*" (OID 2.5.4.10: Nombre de la Organización): DEBE estar presente y DEBE coincidir con el nombre de la Persona Jurídica Pública o Privada responsable del sitio web.

j) "*serialNumber*" (OID 2.5.4.5: Nro. de serie): DEBE estar presente y DEBE contener 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): DEBE estar presente y DEBE representar el país de emisión de los certificados, codificado según el estándar [ISO3166] de DOS (2) caracteres.

Métodos para comprobar la posesión de la clave privada.

Ref: 3.2.1. - Métodos para comprobar la posesión de la clave privada.

No se agrega información.

Autenticación de la identidad de personas jurídicas públicas o privadas.

Ref: 3.2.2. - Autenticación de la identidad de personas jurídicas públicas o privadas.

Para personas jurídicas públicas o privadas:

a) Documento de identidad (original y fotocopia).
b) Nota de confirmación del requerimiento del certificado referida a la persona jurídica solicitante.
c) Acuerdo con Suscriptores firmado
d) Recibo que acredita el pago del certificado correspondiente
e) De tratarse de personas jurídicas privadas, registro con los documentos que se detallan más abajo con copias certificadas por Escribano Público de corresponder:
    a) Estatuto o Contrato Social correspondiente a la Persona Jurídica.

b) Acta de directorio o Poder General Amplio o Poder Especial que autorice la solicitud de certificado de firma digital
c) Constancia de inscripción en el Registro Público de Comercio.
d) Constancia de inscripción en AFIP.
e) Documento Nacional de Identidad de todos los socios, en caso de sociedades irregulares.

f) 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.

Requerimiento de revocación.

Ref: 3.4. - Requerimiento de revocación.

El suscriptor cuando se trate de certificados de persona física o la persona física a cargo de la custodia de la clave privada para el resto de los casos, podrá revocar el certificado digital o pedir la revocación de su certificado a través de alguno de los siguientes medios:

- Por correo electrónico firmado digitalmente a la dirección: revocacion@digilogix.com.ar *que se encuentra disponible las VEINTICUATRO (24) horas del día.*
- Ingresando al sitio web de la **AC – DIGILOGIX** a la siguiente URL: http://www.digilogix.com.ar/suscriptor, *si tiene acceso a su clave privada o utilizando el código de revocación que le fuera informado al momento de la emisión de su certificado.*
- 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.

Solicitud de certificado.

Ref: 4.1.2. - Solicitud de certificado.

Las solicitudes sólo podrán ser iniciadas por el solicitante, en el caso de certificados de personas físicas, por 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 Personas Físicas, 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 física o el representante legal o apoderado en caso de persona jurídica, el Responsable del Servicio, aplicación o sitio web, autorizado a tal fin, en el caso de personas jurídicas debe probar su carácter de suscriptor para esta Política Única de Certificación de acuerdo a lo indicado en el apartado 1.3.3.

El solicitante deberá:

a) Ingresar al sitio web del Certificador http://www.digilogix.com.ar/suscriptor/
b) seleccionando el enlace a la aplicación de solicitud de emisión de certificados
c) Completar la solicitud de certificado con los datos requeridos de acuerdo al tipo de certificado, seleccionando la Autoridad de Registro que le corresponde.
d) Aceptar el Acuerdo con Suscriptores en el que se hace referencia a la Política Única de Certificación que respalda la emisión del certificado.
e) Enviar su solicitud a la **AC - DIGILOGIX** e imprimirla.
f) Presentase ante la Autoridad de Registro correspondiente para realizar la identificación personal y la verificación de la documentación requerida en cada.

Una vez ingresados sus datos y como paso previo a la generación del par de claves, seleccionará el nivel de seguridad del certificado requerido (alto o normal), firma la nota de solicitud del certificado ante el Oficial de Registro de la Autoridad de Registro correspondiente, y quedan aceptadas las condiciones de emisión y uso del certificado.

Procesamiento de la solicitud del certificado.

Ref: 4.2. – Procesamiento de la solicitud del certificado.

El procesamiento de la solicitud finaliza con su aceptación o rechazo por parte de la Autoridad de Registro.

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

- Verifica la existencia de la solicitud en la aplicación del certificador.
- Valida la identidad del solicitante o su representante autorizado mediante la verificación de la documentación requerida
- Verifica la titularidad de la solicitud mediante el control de la nota de solicitud del certificado.
- Requiere al solicitante o su representante autorizado la firma de la nota de solicitud en su presencia
- Resguarda toda la documentación respaldatoria del proceso de validación por el término de DIEZ (10) años a partir de la fecha de vencimiento o revocación del certificado.

Una vez cumplido el proceso de autenticación de la identidad, el solicitante firma la solicitud de su certificado digital ante la Autoridad de Registro correspondiente, con lo que quedan aceptadas las condiciones de emisión y uso del certificado digital.

La solicitud de certificado que no haya finalizado el proceso de identificación, caducará a los TREINTA (30) días de su generación.

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

- Verifica la existencia de la solicitud en la aplicación del certificador.
- Valida la identidad del solicitante o su representante autorizado mediante la verificación de la documentación requerida
- Verifica la titularidad de la solicitud mediante el control de la nota de solicitud del certificado.
- Requiere al solicitante o su representante autorizado la firma de la nota de solicitud en su presencia
- 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.

Proceso de emisión del certificado.

Ref: 4.3.1. – Proceso de emisión del certificado.

No se agrega información.

Notificación de emisión.

Ref: 4.3.2. – Notificación de emisión.

La notificación de la emisión del certificado se efectúa a través de un correo electrónico remitido por la aplicación del certificador a la cuenta de correo declarada por el solicitante o representante autorizado al momento de iniciar el trámite. En dicho correo se indica el link al que deberá acceder el solicitante para descargar el certificado.

Aceptación del certificado.

Ref: 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 vía correo electrónico a la dirección que consignó en la solicitud desde la cuenta certificado@digilogix.com.ar o desde el sitio web.

Procedimientos para la solicitud de revocación.

Ref: 4.9.3. - Procedimientos para la solicitud de revocación.

El suscriptor cuando se trate de certificados de persona física o la persona física a cargo de la custodia de la clave privada para el resto de los casos, podrá revocar el certificado digital o pedir la revocación de su certificado a través de alguno de los siguientes medios:

- Por correo electrónico firmado digitalmente a la dirección: revocacion@digilogix.com.ar *que se encuentra disponible las VEINTICUATRO (24) horas del día.*
- Ingresando al sitio web de la **AC – DIGILOGIX** a la siguiente URL:
- http://www.digilogix.com.ar/suscriptor, *si tiene acceso a su clave privada o utilizando el código de revocación que le fuera informado al momento de la emisión de su certificado.*
- 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.

Frecuencia de emisión de listas de certificados revocados.

Ref: 4.9.7. - Frecuencia de emisión de listas de certificados revocados.

El Certificador 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.

Vigencia de la lista de certificados revocados.

Ref: 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.

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

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

El certificador 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.

El servicio se encuentra disponible SIETE (7) x VEINTICUATRO (24) horas, sujeto a un razonable calendario de mantenimiento, a partir de su sitio web http://www.digilogix.com.ar/ar

Características técnicas.

Ref: 4.10.1. – Características técnicas.

El servicio disponible para la verificación del estado de los certificados emitidos por el certificador es:

- Lista de certificados revocados (CRL)

Respecto a la CRL, se emite cada VEINTICUATRO (24) horas y delta CRLs en modo horario.

Disponibilidad del servicio.

Ref: 4.10.2. – Disponibilidad del servicio.

El servicio se encuentra disponible SIETE (7) x VEINTICUATRO (24) horas, sujeto a un razonable calendario de mantenimiento, a partir de su sitio web http://www.digilogix.com.ar/ar

Aspectos operativos.

Ref: 4.10.3. – Aspectos operativos.

No se agrega información.

Cambio de claves criptográficas.

Ref: 5.6. - Cambio de claves criptográficas.

El par de claves del Certificador ha sido generado con motivo del licenciamiento de la Política única de Certificación y tendrá 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 del certificador implica la emisión de un nuevo certificado por parte de la AC Raíz de la REPÚBLICA ARGENTINA. Si la clave privada del Certificador 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.

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

Generación e instalación del par de claves criptográficas.

Ref: 6.1. - Generación e instalación del par de claves criptográficas.

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 del certificador 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 el Certificador 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.

Ref: 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 de manera tal que su clave privada se encuentre bajo su exclusivo y permanente conocimiento y control. El suscriptor es considerado titular del par de claves; como tal, está obligado a generarlo en un sistema confiable, a no revelar su clave privada a terceros bajo ninguna circunstancia y a almacenarla en un medio que garantice su confidencialidad.

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

El Certificador, 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.

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.

Las claves criptográficas de los suscriptores son generadas por software (nivel de seguridad normal) o por hardware (nivel de seguridad alto) y almacenada por ellos. En este último caso los dispositivos criptográficos utilizados deben ser FIPS 140-2 Nivel 2.

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.

Ref: 6.1.2. – Entrega de la clave privada.
No se agrega información.
.

Ref: 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** utilizará 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 el Certificador se encuentran vinculados a dicha clave pública
- El remitente posee la clave privada que corresponde a la clave pública transferida.

Ref: 6.1.4. - Disponibilidad de la clave pública del certificador.

El certificado de la **AC – DIGILOGIX,** el de la Autoridad Certificante Raíz de la REPÚBLICA ARGENTINA y aquellos emitidos a proveedores de otros servicios de firma digital se encuentran a disposición de los suscriptores y terceros usuarios en su sitio web (http://www.digilogix.com.ar/documentos)

Ref: 6.1.5. - Tamaño de claves.

El Certificador genera su par de claves criptográficas utilizando el algoritmo RSA de 4096 bits.

Los suscriptores, incluyendo las Autoridades de Registro y los Proveedores de otros servicios de firma digital generan sus claves mediante el algoritmo RSA con un tamaño de clave 2048 bits, excepto el caso de las Autoridades de Sello de Tiempo para las que son de 4096 bits.

Ref: 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.

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

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

Ref: 6.2.1. - Controles y estándares para dispositivos criptográficos.

Para la generación y el almacenamiento de las claves criptográficas, el Certificador, las Autoridades de Registro y los suscriptores que opten por un nivel Alto para sus certificados, utilizan los dispositivos referidos en el apartado 6.1.1.

Ref: 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.

Ref: 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.

- Éstos procedimientos sólo puede 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.

Ref: 6.2.4. - Copia de seguridad de clave privada.

El Certificador genera una copia de seguridad de la clave privada a través de un procedimiento que garantiza su integridad y confidencialidad.
No se mantienen copias de las claves privadas de los suscriptores de certificados ni de los Oficiales de Registro.

Ref: 6.2.5. - Archivo de clave privada.

El Certificador almacena las copias de reguardo 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, de acuerdo a lo dispuesto por la Decisión Administrativa Nº 927/14 en cuanto a los niveles de reguardo de claves.

Ref: 6.2.6. - Transferencia de claves privadas en dispositivos criptográficos.

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

Ref: 6.2.7. - Almacenamiento de claves privadas en dispositivos criptográficos.

El almacenamiento de las claves criptográficas del certificador se realiza en el mismo dispositivo de generación que brinda un alto nivel de seguridad de acuerdo a la certificación FIPS 140-2 nivel 3 y nivel 4 de seguridad física de acuerdo a lo establecido en el Anexo II de la Decisión Administrativa JGM N° 927/2014.
Las claves criptográficas de las Autoridades de Registro y de los suscriptores de certificados de nivel de seguridad Alto son almacenadas en el mismo dispositivo criptográfico FIPS 140-2 nivel 2 donde se generan, con los mismos niveles de seguridad.

Ref: 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 descripto más arriba. Estos participantes son autenticados utilizando métodos adecuados de identificación.

Ref: 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.

Ref: 6.2.10. - Método de destrucción de claves privadas.

Las claves privadas de la **AC – DIGILOGIX** se destruyen mediante procedimientos que imposibilitan su posterior recuperación o uso, bajo las mismas medidas de seguridad física que se emplearon para su creación.

Ref: 6.2.11. - Requisitos de los dispositivos criptográficos.

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

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

Los suscriptores que opten por un nivel de seguridad alto, utilizan dispositivos criptográficos FIPS 140-2 Nivel 2.

Los proveedores de otros servicios relacionados con la firma digital utilizan dispositivos criptográficos FIPS 140-2 Nivel 2 como mínimo.

Archivo permanente de la clave pública.

Ref: 6.3.1. - Archivo permanente de la clave pública.

Los certificados emitidos por la **AC - DIGILOGIX** y aquellos emitidos a 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 se almacenan en formato estándar bajo codificación internacional DER.

Generación e instalación de datos de activación

Ref: 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 del certificador 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 el Certificador 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.

Protección de los datos de activación.

Ref: 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.

Otros aspectos referidos a los datos de activación.

Ref: 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.

Requisitos de seguridad computacional.

Ref: 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 2008 R2 Server Enterprise en proceso de evaluación para certificar EAL4+

Windows 2008 Server Enterprise x86: certificado EAL4+

SQL 2008 Enterprise x64 SP1: certificado EAL4+

El dispositivo criptográfico utilizado por el certificador está certificado por el NIST (National Institute of Standards and Technology) FIPS 140-2 Nivel 3.

Los dispositivos criptográficos utilizados por las Autoridades de Registro y por los suscriptores con nivel de seguridad Alto están certificados por NIST (National Institute of Standards and Technology) FIPS 140-2 Nivel 2.

Los dispositivos criptográficos utilizados por las AR y por los suscriptores con nivel de seguridad Alto están certificados por NIST (National Institute of Standards and Technology) FIPS 140-2 Nivel 2.

Controles Técnicos del ciclo de vida de los sistemas.

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

Se implementan 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.

Controles de desarrollo de sistemas.

Ref: 6.6.1. - Controles de desarrollo de sistemas.

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

El Certificador cumple con la separación de ambientes de desarrollo, prueba y producción.

Cumple con el control de versiones para los componentes desarrollados y formaliza pruebas de uso.

Controles de seguridad del ciclo de vida del software.

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

No aplicable.

Certificación de fecha y hora.

.Ref: 6.8. – Certificación de fecha y hora.

El servicio de emisión de sellos de tiempo de la **AC – DIGILOGIX** está basado en la especificación de los estándares RCF 3161 – "Internet X.509 Public Key Infrastructure, ETSI TS 102 023, Time-Stamp Protocol, Electronic Signatures and Infrastructures (ESI) Policy requirements for time-stamping authorities, ETSI TS 101 861, "Time stamping profile" y a su especificación equivalente RFC 3628 – "Requirements for time-stamping authorities"; y está sincronizado con la hora oficial de la REPÚBLICA ARGENTINA.

Perfiles de Certificados y de Listas de Certificados Revocados.

Ref: 7. - Perfiles de certificados y de listas de certificados revocados.

Todos los certificados son emitidos conforme con lo establecido en la especificación ITU X.509 versión 3, y cumplen con las indicaciones establecidas en la sección **"**2 - Perfil de certificados digitales" del Anexo IV - Perfiles de los Certificados y de las Listas de Certificados Revocados.

Perfil del certificado de persona física.

Campos Atributos Extensiones	Valor/OID	Observaciones
Versión (Version)	2	Corresponde a versión 3
Número de serie (SerialNumber)	hasta 20 octetos 2.5.4.5	Entero positivo asignado unívocamente por la AC-DIGILOGIX a cada certificado
Algoritmo de Firma	sha1RSA 1.2.840.113549.1.1.	Algoritmo usado por el certificador para firmar

(SignatureAlgoritm)	5	
Nombre distintivo del emisor (Issuer)		
commonName	AC-DIGILOGIX 2.5.4.3	Identificación de la Autoridad Certificante
serialNumber	30714128716 2.5.4.5	CUIT del Certificador
organizationName	DIGILOGIX S.A. 2.5.4.10	Denominación del Certificador Licenciado
stateOrProvinceName	Ciudad Autónoma de Buenos Aires 2.5.4.8	Ciudad en la que se encuentra el Certificador
countryName	AR 2.5.4.6	País del Certificador Licenciado
Validez (desde, hasta) (Validity (Not before, not after))		
notBefore	<fecha y hora de emisión UTC> yyyy/mm/dd hh:mm:ss huso-horario	Fecha y hora en que el período de vigencia del certificado comienza
notAfter	<fecha y hora de emisión UTC+ 1 año> yyyy/mm/dd hh:mm:ss huso-horario	Fecha y hora en que el periodo de vigencia del certificado termina
Nombre distintivo del suscriptor (Subject)		
commonName	<Nombres y Apellidos> 2.5.4.3	Datos que surgen del Documento Nacional de Identidad presentado por el titular
serialNumber	<Tipo> <Número de documento> 2.5.4.5	Datos que surgen del Documento presentado por el titular
title	<Nombre de la función> 2.5.4.12	Cargo o título del suscriptor dentro de la organización, debe corresponder con la certificación aportada en el proceso de autenticación
organizationName	<Nombre de la empresa u organismo> 2.5.4.10	Nombre que surge de la certificación aportada en el proceso de autenticación
localityName	<Nombre de localidad> 2.5.4.7	Nombre que surge de la certificación aportada en el proceso de autenticación
stateOrProvinceName	<Nombre de la provincia> 2.5.4.8	Nombre que surge de la certificación aportada en el proceso de autenticación
countryName	AR	Código de País de acuerdo a ISO3166

	2.5.4.6	
Clave pública del suscriptor (Subject Public Key Info)		
public key algorithm	RSA 1.2.840.11.35.49.1.1.1	Tipo de algoritmo de clave pública utilizado
Public key length	1024 bits	Longitud de la clave pública del suscriptor
Clave pública del suscriptor (Subject Public Key Info)	<Clave pública del suscriptor>	Valor de la clave pública del suscriptor
Extensiones del certificado (Extensions)		
Restricciones básicas (Basic Constraints)	Tipo de asunto = Entidad final pathLenghtConstraint = Null 2.5.29.19	Define el certificado como de entidad final
Usos de clave (Key Usage)	digitalSignature = 1 nonRepudiation = 1 keyEncipherment = 0 dataEncipherment = 0 keyAgreement = 0 keyCertSign = 0 cRLSign = 0 encipherOnly = 0 decipherOnly = 0 2.5.29.15	Propósito para el cual será utiliza la clave contenida en el certificado. Sin repudio, firma digital
Identificador de clave del Suscriptor (Subject Key Identifier)	Valor de hash de 20 bytes 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 (CRLDistribution Points)	[1]Punto de distribución CRL Dirección URL=http://www.digilogix.com.ar/crl/digilogix.crl [2]Punto de distribución CRL Dirección URL= http://backup.digilogix.com.ar/crl/digilogix.crl 2.5.29.31	URI del punto de distribución
Política de Certificación (Certificate Policies)	OID de la Política de Certificación de DIGILOGIX S.A, URI de la Política: http://www.digilogix.com.ar /documentos/cps.pdf Texto de aviso=certificado emitido por un certificador licenciado en el marco de la Ley 25.506	OID de la Política de Certificación de DIGILOGIX S.A, otorgado por la ONTI, URI de la Política de Certificación y texto obligatorio para los certificados de la IFDRA

Identificador de la Clave de la Autoridad Certificante (AuthorityKeyIdentifier)	Valor de hash de 20 bytes 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)	Autenticación del cliente (1.3.6.1.5.5.7.3.2) Correo seguro (1.3.6.1.5.5.7.3.4) 2.5.29.37	Usos adicionales de la clave pública a los enumerados en el campo keyUsage
Nombres Alternativos del Suscriptor (Subject Alternative Name)	<Dirección de correo electrónico> 2.5.29.17	Dirección de mail del suscriptor verificada por circuito seguro compatible con RFC 822

Perfil del certificado de la persona jurídica.

Campos Atributos Extensiones	Valor/OID	Observaciones
Versión (Version)	2	Corresponde a versión 3
Número de serie (SerialNumber)	hasta 20 octetos 2.5.4.5	Entero positivo asignado unívocamente por la AC-DIGILOGIX a cada certificado
Algoritmo de Firma (Signature)	sha1RSA 1.2.840.113549.1.1.5	Algoritmo usado por el certificador para firmar
Nombre distintivo del emisor (Issuer)		
commonName	AC-DIGILOGIX 2.5.4.3	Identificación de la Entidad Certificante
serialNumber	30714128716 2.5.4.5	CUIT del Certificador
organizationName	DIGILOGIX S.A. 2.5.4.10	Denominación del Certificador Licenciado
stateOrProvinceName	Ciudad Autónoma de Buenos Aires 2.5.4.8	Ciudad en la que se encuentra el Certificador
countryName	AR 2.5.4.6	País del Certificador Licenciado
Validez (desde, hasta) (Validity (Not before, not after))		
notBefore	<fecha y hora de emisión UTC>	Fecha y hora en que el período de vigencia del certificado comienza

	yyyy/mm/dd hh:mm:ss huso-horario	
notAfter	<fecha y hora de emisión UTC+3 años> yyyy/mm/dd hh:mm:ss huso-horario	Fecha y hora en que el periodo de vigencia del certificado termina
Nombre distintivo del suscriptor (Subject)		
commonName	Unidad Operativa del Suscriptor 2.5.4.3	Denominación de la Unidad Operativa del Suscriptor
serialNumber	CUIT <Número de CUIT> 2.5.4.5	CUIT de la Persona Jurídica
organizationName	<Nombre de la empresa u organismo> 2.5.4.10	Nombre que surge de la certificación aportada por el representante autorizado durante el proceso de autenticación
localityName	<Nombre de localidad> 2.5.4.7	Nombre que surge de la certificación aportada en el proceso de autenticación
stateOrProvinceName	<Nombre de la provincia> 2.5.4.8	Nombre que surge de la certificación aportada en el proceso de autenticación
countryName	AR 2.5.4.6	
Clave pública del suscriptor (Subject Public Key Info)		
public key algorithm	RSA 1.2.840.11.35.49.1.1 .1	Tipo de algoritmo de clave pública utilizado
Public key length	1024 bits	Longitud de la clave pública del suscriptor
Subject Public Key Info	<Clave pública del suscriptor>	Valor de la clave pública del suscriptor
Extensiones del certificado (Extensions)		
Restricciones básicas (Basic Constraints)	Tipo de asunto = Entidad final pathLenghtConstraint = Null 2.5.29.19	Define el certificado como de entidad final
Usos de clave (Key Usage)	digitalSignature = 1 nonRepudiation = 1 keyEncipherment = 0 dataEncipherment = 0 keyAgreement = 0 keyCertSign = 0 cRLSign = 0 encipherOnly = 0 decipherOnly = 0	Sin repudio, firma digital

	2.5.29.15	
Identificador de clave del Suscriptor (Subject Key Identifier)	Valor de hash de 20 bytes 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)	[1]Punto de distribución CRL Dirección URL=http://www.digilogix.com.ar/crl/digilogix.crl [2]Punto de distribución CRL Dirección URL= http://backup.digilogix.com.ar/crl/digilogix.crl 2.5.29.31	URI del punto de distribución
Política de Certificación (Certification Policies)	OID de la Política de Certificación de DIGILOGIX S.A, URI de la Política: http://www.digilogix.com.ar/documentos/cps.pdf Texto de aviso=certificado emitido por un certificador licenciado en el marco de la Ley 25.506	OID de la Política de Certificación de DIGILOGIX S.A, otorgado por la ONTI, URI de la Política de Certificación y texto obligatorio para los certificados de la IFDRA
Identificador de la Clave de la Autoridad Certificante (AuthorityKeyIdentifier)	Valor de hash de 20 bytes 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)	Autenticación del cliente (1.3.6.1.5.5.7.3.2) Correo seguro (1.3.6.1.5.5.7.3.4) 2.5.29.37	Usos adicionales de la clave pública a los enumerados en el campo keyUsage
Nombres Alternativos del Suscriptor (Subject Alternative Name)		

commonName	Nombres y Apellidos 2.5.4.3	Datos que surgen del Documento Nacional de Identidad presentado por el titular
serialNumber	<Tipo> <Número de documento> 2.5.4.5	Datos que surgen del Documento Nacional de Identidad presentado por el titular
title	<Nombre de la función> 2.5.4.12	Cargo o título del suscriptor dentro de la organización, debe corresponder con la certificación aportada en el proceso de autenticación

Perfil del certificado de aplicaciones.

Certificado x.509 v3 Atributos Extensiones	**Nombre del campo y OID**	**Contenido**
Versión (Version)	2	V3 2 (correspondiente a versión 3)
Número de serie (SerialNumber)	Serial Number 2.5.4.5	<Número de serie del certificado> (entero positivo asignado unívocamente por la AC DIGILOGIX a cada certificado de hasta 20 octetos)
Algoritmo de Firma (SignatureAlgoritm)	1.2.840.113549.1.1.5	sha1RSA
Nombre distintivo del emisor (Issuer)	AC DIGILOGIX - 2.5.4.3	CN=Autoridad Certificante de Firma Digital
	30714128716 2.5.4.5	SERIAL NUMBER=CUIT 30714128716
	DIGILOGIX S.A. - 2.5.4.10	Denominación del Certificador Licenciado
	organizationalUnitName - 2.5.4.11	OU= DIGILOGIX S.A
	stateOrProvinceName - 2.5.4.8	S=Ciudad Autónoma de Buenos Aires
	countryName - 2.5.4.6	C=AR
Validez (desde, hasta)	notBefore	<fecha y hora de emisión UTC> yyyy/mm/dd hh:mm:ss huso-horario
	notAfter	<fecha y hora de emisión UTC+ 3 años> yyyy/mm/dd hh:mm:ss huso-horario
Nombre distintivo del suscriptor (Subject DN)	commonName - 2.5.4.3	CN=Denominación de la Aplicación
	organizationName 2.5.4.10	O=nombre de la Persona Jurídica Pública o Privada responsable de la aplicación

	organizationalUnitName 2.5.4.11	OU=Unidad Operativa relacionada con la aplicación
	serialNumber - 2.5.4.5	SN= <CUIT/CUIL> <Número de la Persona Jurídica Pública o Privada responsable de la aplicación>
	countryName - 2.5.4.6	C=AR
Clave pública del suscriptor (Subject Public Key Info)	public key algorithm 1.2.840.11.35.49.1.1.1	RSA
	Public key length	2048 bits
	Clave pública del suscriptor	<Clave pública del suscriptor>
0…….Restricciones básicas (Basic Constraints)	basicConstraint 2.5.29.19	Tipo de asunto = Entidad final pathLenghtConstraint = Null
Usos de clave (Key Usage)	keyUsage 2.5.29.15	digitalSignature = 1 contentCommitment = 1 keyEncipherment = 1 dataEncipherment = 1 keyAgreement = 1 keyCertSign = 0 cRLSign = 0 encipherOnly = 1 decipherOnly = 1
Identificador de clave del suscriptor (Subject Key Identifier)	(Subject Key Identifier)	Contiene un hash de 20 bytes del atributo clave pública del suscriptor
Puntos de Distribución de la Lista de Certificados Revocados (CRLDistributionPoints)	CRLDistributionPoints - 2.5.29.31	[1]Punto de distribución CRL Nombre del punto de distribución: Nombre completo: Dirección URL=http://www.digilogix.com.ar/crl/digilogix.crl Dirección URL=http://backup.digilogix.com.ar/crl/digilogix.crl

Política de Certificación		[1]Política de certificación: OID de la Política Única =2.16.32.1.1.3 [1.1] Información de la Política de Certificación: Id. De la Política de Certificación =CPS Ubicación: http://www.digilogix.com.ar/documentos/cps.pdf User notice = certificado emitido por un certificador licenciado en el marco de Ley 25.506.
Identificador de la Clave de la Autoridad Certificante (AuthorityKeyIdentifier)	AuthorityKeyIdentifier 2.5.29.35	keyIdentifier = <Identificador de la clave de la AC> (Contiene un hash de 20 bytes del atributo clave pública de la AC DIGILOGIX)
Uso Extendido de Clave (Extended Key Usage)	ExtendedKeyUsage 2.5.29.37	Autenticación del cliente (1.3.6.1.5.5.7.3.2)
Nombres Alternativos del Suscriptor (Subject Alternative Name)	SubjectAltName 2.5.29.17	CN=APELLIDO Nombre de la persona física a cargo de la custodia de la clave privada. SN= <CUIT/CUIL> <Número> OID=2.5.4.12 T=<Relación que vincula a la persona física con la persona jurídica>
Información de Acceso de la AC (Authority Information Access)	1.3.6.1.5.5.7.48.1	URL=http://www.digilogix.com.ar/ar
Declaración del certificado calificado	2.16.32.1.10.1	claves generadas por software

(QCStatment)		

Perfil del certificado de proveedores de servicios de firma digital.
Para Autoridad de Competencia.

Certificado x.509 v3 Atributos Extensiones	**Nombre del campo y OID**	**Contenido**
Versión (Version)	2	V3 2 (correspondiente a versión 3)
Número de serie (SerialNumber)	Serial Number 2.5.4.5	<Número de serie del certificado> (entero positivo asignado unívocamente por la AC DIGILOGIX a cada certificado de hasta 20 octetos)
Algoritmo de Firma (SignatureAlgoritm)	1.2.840.113549.1.1.5	sha1RSA
Nombre distintivo del emisor (Issuer)	commonName - 2.5.4.3	CN=Autoridad Certificante de Firma Digital
	serialNumber - 2.5.4.5	CUIT 30714128716
	organizationName - 2.5.4.10	O=DIGILOGIX S.A.
	organizationalUnitName - 2.5.4.11	OU=AC - DIGILOGIX
	stateOrProvinceName - 2.5.4.8	S=Ciudad Autónoma de Buenos Aires
	countryName - 2.5.4.6	C=AR
Validez (desde, hasta)	notBefore	<fecha y hora de emisión UTC> yyyy/mm/dd hh:mm:ss huso-horario
	notAfter	<fecha y hora de expiración a establecer por AC DIGILOGIX> yyyy/mm/dd hh:mm:ss huso-horario
Nombre distintivo del suscriptor (Subject DN)	commonName - 2.5.4.3	CN=Denominación del servicio de emisión de sello de competencia
	organizationalUnitName 2.5.4.11	OU=Unidad Operativa relacionada con el suscriptor
	organizationName	O=Nombre de la Persona Jurídica Pública o Privada responsable
	2.5.4.10	del servicio
	serialNumber - 2.5.4.5	SN= <CUIT/CUIL> <Número de la Persona Jurídica Pública o Privada>
	countryName - 2.5.4.6	C=AR
Clave pública del suscriptor (Subject Public Key Info)	public key algorithm 1.2.840.11.35.49.1.1.1	RSA

	Public key length	2048 bits
	Clave pública del suscriptor	<Clave pública del suscriptor>
Restricciones básicas (Basic Constraints)	basicConstraint 2.5.29.19	Tipo de asunto = Entidad final pathLenghtConstraint = Null
Usos de clave (Key Usage)	keyUsage 2.5.29.15	digitalSignature = 1 contentCommitment = 1 keyEncipherment = 0 dataEncipherment = 0 keyAgreement = 0 keyCertSign = 0 cRLSign = 1 encipherOnly = 0 decipherOnly = 0
Identificador de clave del suscriptor (Subject Key Identifier)	(Subject Key Identifier)	Contiene un hash de 20 bytes del atributo clave pública del suscriptor
Puntos de Distribución de la Lista de sellos de competencia Revocados (CRLDistributionPoints)	CRLDistributionPoints - 2.5.29.31	[1]Punto de distribución CRL Nombre del punto de distribución: Nombre completo: Dirección URL=http://www.digilogix.com.ar/crl/digilogix.crl Dirección URL=http://backup.digilogix.com.ar/crl/digilogix.crl
Política de Certificación		[1]Política de certificación: OID de la Política Única =2.16.32.1.1.3 [1.1] Información de la Política de Certificación: Id. De la Política de Certificación =CPS Ubicación: http://www.digilogix.com.ar/documentos/cps.pdf User notice = certificado emitido por un certificador licenciado en el marco de Ley 25.506.
Identificador de la Clave de la Autoridad Certificante (AuthorityKeyIdentifier)	AuthorityKeyIdentifier 2.5.29.35	keyIdentifier = <Identificador de la clave de la AC> (Contiene un hash de 20 bytes del atributo clave pública de la AC DIGILOGIX)
Uso Extendido de Clave (Extended Key Usage)	ExtendedKeyUsage 2.5.29.37	Autenticación del cliente (1.3.6.1.5.5.7.3.2)

Información de Acceso de la AC (Authority Information Access)	1.3.6.1.5.5.7.48.1	URL=http://digilogix.com.ar/ar

Para Autoridad de Sello de Tiempo.

Certificado x.509 v3 Atributos Extensiones	**Nombre del campo y OID**	**Contenido**
Versión (Version)		V3 2 (correspondiente a versión 3)
Número de serie (SerialNumber)	Serial Number 2.5.4.5	<Número de serie del certificado> (entero positivo asignado unívocamente por la AC DIGILOGIX a cada certificado de hasta 20 octetos)
Algoritmo de Firma (SignatureAlgoritm)	1.2.840.113549.1.1.5	sha1RSA
Nombre distintivo del emisor (Issuer)	commonName - 2.5.4.3	CN=Autoridad Certificante de Firma Digital
	serialNumber - 2.5.4.5	SERIALNUMBER=CUIT 30714128716
	organizationName - 2.5.4.10	O= DIGILOGIX S.A.
	organizationalUnit	OU=AC DIGILOGIX
	Name - 2.5.4.11	
	stateOrProvinceName - 2.5.4.8	S=Ciudad Autónoma de Buenos Aires
	countryName - 2.5.4.6	C=AR
Validez (desde, hasta)	notBefore	<fecha y hora de emisión UTC> yyyy/mm/dd hh:mm:ss huso-horario
	notAfter	<fecha y hora de expiración a establecer por AC DIGILOGIX yyyy/mm/dd hh:mm:ss huso-horario

Nombre distintivo del suscriptor (Subject DN)	commonName - 2.5.4.3	CN=Denominación del servicio de emisión de sello de tiempo
	organizationalUnit Name 2.5.4.11	OU=Unidad Operativa relacionada con el suscriptor
	organizationName 2.5.4.10	O=Nombre de la Persona Jurídica Pública o Privada responsable del servicio
	serialNumber - 2.5.4.5	SN= <CUIT/CUIL> <Número de la Persona Jurídica Pública o Privada>
	countryName - 2.5.4.6	C=AR
Clave pública del suscriptor (Subject Public Key Info)	public key algorithm 1.2.840.11.35.49.1.1.1	RSA
	Public key length	2048 bits
	Clave pública del suscriptor	<Clave pública del suscriptor>
Restricciones básicas (Basic Constraints)	basicConstraint 2.5.29.19	Tipo de asunto = Entidad final pathLenghtConstraint = Null
Usos de clave (Key Usage)	keyUsage 2.5.29.15	digitalSignature = 1 contentCommitment = 1 keyEncipherment = 0 dataEncipherment = 0 keyAgreement = 0 keyCertSign = 0 cRLSign = 0 encipherOnly = 0 decipherOnly = 0
Identificador de clave del suscriptor (Subject Key Identifier)	(Subject Key Identifier)	Contiene un hash de 20 bytes del atributo clave pública del suscriptor
Puntos de Distribución de la Lista de sellos de tiempo Revocados (CRLDistributionPoints)	CRLDistributionPoints - 2.5.29.31	[1]Punto de distribución CRL Nombre del punto de distribución: Nombre completo: Dirección URL=http://www.digilogix.com.ar/crl/digilogix.crl [[2]Punto de distribución CRL Dirección URL= http://backup.digilogix.com.ar/crl/digilogix.crl

Política de Certificación		[1]Política de certificación: OID de la Política Única =2.16.32.1.1.3 [1.1] Información de la Política de Certificación: Id. De la Política de Certificación =CPS Ubicación: http://digilogix.com.ar/documentos/cps.pdf User notice = certificado emitido por un certificador licenciado en el marco de Ley 25.506.
Identificador de la Clave de la Autoridad Certificante (AuthorityKeyIdentifier)	AuthorityKeyIdentifier 2.5.29.35	keyIdentifier = <Identificador de la clave de la AC> (Contiene un hash de 20 bytes del atributo clave pública de la AC DIGILOGIX)
Uso Extendido de Clave (Extended Key Usage)	ExtendedKeyUsage 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)
Declaración del certificado calificado (QCStatment)		OID= 2.16.32.1.10.2.2 (claves generadas por disp. FIPS 140-2 nivel 2) OID= 2.16.32.1.10.2.3 (claves generadas por disp. FIPS 140-2 nivel 3)

Perfil de la lista de certificados revocados.

.Campos Atributos Extensiones	Valor/OID	Observaciones
Versión (Version)	1	Corresponde a versión 2
Algoritmo de Firma (Signature)	sha1RSA 1.2.840.113549.1.1.5	Algoritmo usado por el certificador para firmar
Nombre distintivo del emisor (Issuer)		
commonName	AC-DIGILOGIX 2.5.4.3	Identificación de la Entidad Certificante
serialNumber	30714128716 2.5.4.5	CUIT del Certificador
organizationName	DIGILOGIX S.A. 2.5.4.10	Denominación del Certificador Licenciado
stateOrProvinceName	Ciudad Autónoma de Buenos Aires 2.5.4.8	Ciudad en la que se encuentra el Certificador
countryName	AR 2.5.4.6	País del Certificador Licenciado

Día y hora de vigencia (thisUpdate)	<fecha y hora UTC> yyyy/mm/dd hh:mm:ss huso-horario	Fecha y hora efectivas de emisión, a partir de la cual entre en vigencia
Próxima Actualización (nextUpdate)	<fecha y hora UTC> yyyy/mm/dd hh:mm:ss huso-horario	Fecha y hora de emisión de la próxima Lista de Certificados Revocados
Identificador de la Clave de la Autoridad Certificante (AuthorityKeyIdentifier)	Valor de hash de 20 bytes 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)	Número de la CRL OID - 2.5.29.20	Número incremental que identifica la CRL emitida
Indicador Delta CRL (Delta CRL Indicator)	Número de Delta CRL 2.5.29.27	Número que se incrementa cada vez que se emite una Delta CRL
Certificados Revocados (Revoked Certificates)		
Fecha de Revocación	<fecha y hora UTC> yyyy/mm/dd hh:mm:ss huso-horario	Fecha y hora en que se revocó el certificado
Número de Serie del Certificado revocado (Serial Number)	hasta 20 octetos 2.5.4.5	Número de Serie del Certificado revocado
Motivo de la Revocación (ReasonCode) 2.5.29.21	Motivo de acuerdo al RFC 5280	Motivo de la Revocación
Versión de CA	V0.0	Versión de CA

Auditoría de Cumplimiento y Otras Evaluaciones.

Ref: 8. – Auditoría de cumplimiento y otras evaluaciones.

- En base a lo dispuesto por las normas vigentes, **DIGILOGIX S.A**., en su calidad de certificador licenciado se encuentra sujeta a las auditorías que llevan a cabo las siguientes entidades pertenecientes al Sector Público:

  - Ente Licenciante de la Infraestructura Nacional de Firma Digital de la REPÚBLICA ARGENTINA.

- Programa Nacional de Infraestructuras Críticas de Información y Ciberseguridad de la Oficina Nacional de Tecnologías de Información de la SUBSECRETARÍA DE TECNOLOGÍAS DE GESTIÓN de la SECRETARÍA DE GABINETE Y COORDINACIÓN ADMINISTRATIVA de la JEFATURA DE GABINETE DE MINISTROS.

Aranceles.

Ref: 9.1. – Aranceles.

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

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

Responsabilidad Financiera.

Ref: 9.2. - Responsabilidad Financiera.

Las responsabilidades financieras se originan en lo establecido por la Ley N° 25.506 y su Decreto Reglamentario Nº 2628/02 y en las disposiciones de la presente Política.

Confidencialidad.

Ref: 9.3. - Confidencialidad.

Toda información referida a solicitantes o suscriptores de certificados que sea recibida por el Certificador o por las Autoridades de Registro operativamente vinculadas, será tratada en forma confidencial y no puede hacerse pública sin el consentimiento previo de los titulares de los datos, salvo que sea requerida judicialmente. La exigencia se extiende a toda otra información referida a los solicitantes y los suscriptores de certificados a la que tenga acceso el Certificador o sus Autoridades de Redgistro durante el ciclo de vida del certificado.

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

Información confidencial.

Ref: 9.3.1. - Información confidencial.

Toda información remitida por el solicitante o suscriptor de un certificado al momento de efectuar un requerimiento es considerada confidencial y no es divulgada a terceros sin su consentimiento previo y expreso, salvo que sea requerida mediante resolución fundada en causa judicial por juez competente. La exigencia se extenderá también a toda otra información referida a los suscriptores de certificados a la que tenga acceso el certificador o la Autoridad de Registro durante el ciclo de vida del certificado.

El 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 el Certificador.
- Almacenada en cualquier soporte, incluyendo aquella que se trasmita verbalmente, vinculada a procedimientos de certificación, excepto aquella declarada como no confidencial en forma expresa.
- Relacionada con los Planes de Contingencia, controles, procedimientos de seguridad y registros de auditoría pertenecientes al Certificador.

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

Responsabilidades de los roles involucrados

Ref: 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 el Certificador hubiera obtenido autorización expresa de su titular.

Derechos de Propiedad Intelectual.

Ref: 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.

Responsabilidades y garantías.

Ref: 9.6. – Responsabilidades y garantías.

Siempre que sea aplicable, y sin perjuicio de lo determinado por la Ley Nº 25.506 al respecto, las limitaciones de responsabilidad del certificador licenciado se rigen por lo establecido en el art. 39 de la Ley N° 25.506 y sus modificatorias y su Decreto reglamentario Nº 2628/02 y modificatorios, en las disposiciones de la presente Política y en el Acuerdo con suscriptores.

Deslinde de responsabilidad.

Ref: 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.

Limitaciones a la responsabilidad frente a terceros.

Ref: 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.

Compensaciones por daños y perjuicios.

Ref: 9.9. - Compensaciones por daños y perjuicios.

No se agrega información.

Condiciones de vigencia.

Ref: 9.10. - Condiciones de vigencia.

La presente Política Única de Certificación se encuentra vigente a partir de la fecha de su aprobación por parte del Ente Licenciante y 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.

Gestión del ciclo de vida del documento.

Ref: 9.12.- Gestión del ciclo de vida del documento.

No se agrega información.

Procedimientos de cambio.

Ref: 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, artículo 21, inciso q) y por la Decisión Administrativa JGM N° 927/2014 y sus anexos respectivos.

Toda Política Única de Certificación es sometida a aprobación del ente licenciante durante el proceso de licenciamiento.

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 Certificador y sus nuevas versiones se pondrán en vigencia, previa aprobación del ente licenciante.

Mecanismo y plazo de publicación y notificación.

Ref: 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 http://www.digiñogix.com.ar/documentos

Procedimientos de resolución de conflictos.

Ref: 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° 1759/72.

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

Los titulares de certificados y los terceros usuarios podrán interponer ante el ente licenciante recurso administrativo por conflictos referidos a la prestación del servicio por parte del Certificador. Una vez agotada la vía administrativa, podrá interponerse acción judicial, siendo competente la Justicia en lo Contencioso Administrativo Federal.

El reclamo efectuado por un tercero usuario o por el titular de un certificado digital expedido por el Certificador, sólo será procedente previa acreditación de haberse efectuado reclamo ante este último con resultado negativo. Acreditada dicha circunstancia, el ente licenciante procederá a recibir, evaluar y resolver las denuncias mediante la instrucción del correspondiente trámite administrativo.

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

a) Una vez recibido el reclamo en las oficinas del Certificador, este citará al reclamante a una audiencia y labrará un acta que deje expresa constancia de los hechos que

motivan el reclamo y de todas y cada uno de los antecedentes que le sirvan de causa.

b) Una vez que el Certificador emita opinión, se notificará al reclamante y se le otorgará un plazo de CINCO (5) días hábiles administrativos para ofrecer y producir la prueba de su descargo.
c) DIGILOGIX resolverá en un plazo de DIEZ (10) días lo que estime corresponder, dictando el Acto Administrativo correspondiente, conforme a los criterios de máxima razonabilidad, equidad y pleno ajuste al bloque de legalidad vigente y aplicable.

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

El suscriptor o los terceros usuarios podrán accionar ante el ente licenciante, previo agotamiento del procedimiento ante el certificador licenciado correspondiente, el cual deberá proveer obligatoriamente al interesado de un adecuado procedimiento de resolución de conflictos.

Conformidad con normas aplicables.

Ref: 9.15. – Conformidad con normas aplicables.

La legislación que respalda la interpretación, aplicación y validez de esta Política Única de Certificación es la Ley Nº 25.506, el Decreto Nº 2628/02, la Decisión Administrativa Nº 927/14 y toda otra norma complementaria dictada por la autoridad competente.

Otras cuestiones generales.

Ref: 9.17. – Otras cuestiones generales.

No se agrega información.