MANUAL DE PROCEDIMIENTOS

POLÍTICA ÚNICA DE CERTIFICACIÓN

CERTIFICADOR LICENCIADO

LAKAUT S.A.

Versión 2.0

Versión Pública según Política Única de certificación

Tabla de contenido

INTRODUCCIÓN. 5

DESCRIPCIÓN GENERAL. 5

IDENTIFICACIÓN. 5

PARTICIPANTES Y APLICABILIDAD. 6

Certificador *6*

Autoridades de Registro (AR). *6*

Suscriptores de certificados. *8*

Terceros Usuarios. *8*

USO DE LOS CERTIFICADOS. 8

ADMINISTRACIÓN DE LA POLÍTICA 9

Responsable del Documento. *9*

Contacto. *9*

Procedimiento de aprobación de la Política Única de Certificación. *9*

DEFINICIONES Y ACRÓNIMOS. 9

Definiciones. *9*

Acrónimos. *12*

RESPONSABILIDADES VINCULADAS A LA PUBLICACIÓN Y A LOS REPOSITORIOS. 12

REPOSITORIOS. 12

PUBLICACIÓN DE INFORMACIÓN DEL CERTIFICADOR. 13

FRECUENCIA DE PUBLICACIÓN. 13

CONTROLES DE ACCESO A LA INFORMACIÓN 14

IDENTIFICACIÓN Y AUTENTICACIÓN. 14

ASIGNACIÓN DE NOMBRES DE SUSCRIPTORES. 16

Tipos de nombres. *16*

Necesidad de Nombres Distintivos. *16*

Anonimato o uso de seudónimos. *16*

Reglas para la interpretación de nombres. *16*

Unicidad de nombres. *17*

Reconocimiento, autenticación y rol de las marcas registradas. *17*

REGISTRO INICIAL. 17

Autenticación de la identidad de Personas Jurídicas Públicas o Privadas. *17*

Autenticación de la identidad de Personas Físicas. *19*

Información no verificada del suscriptor. *20*

Validación de autoridad. *22*

Criterios para la interoperabilidad. *22*

REQUERIMIENTO DE REVOCACIÓN. 22

CICLO DEL CERTIFICADO: REQUERIMIENTOS OPERATIVOS. 22

SOLICITUD DE CERTIFICADO. 22

ACEPTACIÓN DEL CERTIFICADO. 35

USOS DEL PAR DE CLAVES Y DEL CERTIFICADO. 35

Uso de la clave privada y del certificado por parte del suscriptor. *35*

Uso de la clave pública y del certificado por parte de Terceros Usuarios. *35*

RENOVACIÓN DEL CERTIFICADO. 36

MODIFICACIÓN DEL CERTIFICADO. 36

SUSPENSIÓN Y REVOCACIÓN DE CERTIFICADOS. 36

Causas de Revocación. *37*

Autorizados a solicitar la revocación. *38*

Procedimientos para la solicitud de revocación. *38*

Revocación a solicitud del titular del certificado digital. *39*

Revocación por parte de la AC – LAKAUT. *40*

Plazo para la solicitud de revocación. *41*

Plazo para el procesamiento de la solicitud de revocación. *41*

Requisitos para la verificación de la lista de certificados revocados. *41*

Frecuencia de emisión de listas de certificados revocados. *41*

Vigencia de la lista de certificados revocados. *42*

Disponibilidad del servicio de consulta sobre revocación y de estado del certificado. *42*

Requisitos para la verificación en línea del estado de revocación. *43*

Otras formas disponibles para la divulgación de la revocación. *44*

Requisitos específicos para casos de compromiso de claves. *44*

Causas de suspensión. *44*

Autorizados a solicitar la suspensión. *44*

Procedimientos para la solicitud de suspensión. *45*

Límites del periodo de suspensión de un certificado. *45*

DESVINCULACIÓN DEL SUSCRIPTOR. 45

RECUPERACIÓN Y CUSTODIA DE CLAVES PRIVADAS. 45

5. - CONTROLES DE SEGURIDAD FÍSICA, OPERATIVOS Y DE GESTIÓN. ..... ¡ERROR! MARCADOR NO DEFINIDO.

INTRODUCCIÓN.

Descripción general.

El presente manual establece los procedimientos relacionados con la emisión y administración de los certificados digitales de la Autoridad Certificante de **LAKAUT S.A.** (en adelante "**AC – LAKAUT**"). Dichos procedimientos requieren para su ejecución las funciones instrumentadas por el Sistema Informático de **AC – LAKAUT**, desarrollado por **LAKAUT S.A.**

Este Manual de Procedimientos forma parte de la documentación técnica emitida por la Autoridad Certificante **LAKAUT** (en adelante **AC - LAKAUT**) junto con los siguientes documentos:

a) Política de Certificación

b) Plan de Seguridad

c) Plan de Contingencias

d) Plan de Cese de Actividades

Identificación.

a) Nombre: Manual de Procedimientos de **LAKAUT S.A**.

b) Versión: 2.0

c) Fecha de aplicación: 12-Dic-2015.

d) OID: 2.16.32.1.1.5

e) Lugar o sitio de publicación: se publica en el sitio web de la **AC – LAKAUT**

f) https://www.lakautac.com.ar/

g) Revisión: Responsable de la AC

Participantes y aplicabilidad.

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

b) Las Autoridades de Registro (en adelante AR) que se constituyan en el ámbito de la Política de Certificación para personas físicas y jurídicas que intervengan en procesos de gestión documental, entre otros.

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

d) Los terceros usuarios que verifican firmas digitales basadas en certificados digitales emitidos por el Certificador, en el ámbito de la mencionada Política.

Este Manual de Procedimientos es aplicable a:

Certificador

Los procedimientos descriptos en el presente manual en sus partes pertinentes, son de aplicación obligatoria para **LAKAUT S.A**. en su carácter de certificador licenciado quien emite certificados digitales para personas físicas y jurídicas.

Autoridades de Registro (AR).

Los procedimientos descriptos en el presente manual en sus partes pertinentes, son de aplicación obligatoria para las Autoridades de Registro.

Las Autoridades de Registro realizan las funciones de verificación de identidad de los solicitantes de certificados digitales y la gestión de trámites asociados.

La **AC – LAKAUT** instrumenta un módulo que se corresponde con las funciones de las Autoridades de Registro y es operado por los Oficiales de Registro designados.

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

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

b) Autoridades de Registro Delegadas: la **AC – LAKAUT** admite la constitución de Autoridades de Registro externas al ámbito físico donde desarrolla sus actividades, de

manera que se encuentren en condiciones de efectuar un adecuado control de identidad de los suscriptores de certificados que les presentaran una solicitud de emisión, dado el tipo de información que manejan y su cercanía al usuario final.

En todos los casos, es atribución de la **AC – LAKAUT** autorizar el funcionamiento de las mencionadas Autoridades de Registro Delegadas, a través de la habilitación correspondiente mediante decisión firmada del responsable de la **AC – LAKAUT** en base a un contrato previamente firmado entre **LAKAUT S.A.** y la organización en la que se constituya la Autoridad de Registro.

Estas Autoridades de Registro Delegadas operarán bajo el estricto control y supervisión de la Autoridad de Registro Central de **LAKAUT S.A**.

El contrato referido contendrá como mínimo la siguiente información:

a. Denominación de las partes
b. Domicilio donde desarrollará su actividad la Autoridad de Registro Delegada
c. Datos de contacto de las partes
d. Derechos y obligaciones de la Autoridad de Registro Delegada y del certificador licenciado.
e. Plazo de duración del convenio
f. Causales de cese de la relación
g. Condiciones de prórroga
h. Datos de los firmantes (nombre y apellido, documento de identidad, carácter de representación)

El contrato deberá ser firmado por las máximas autoridades de **LAKAUT S.A.** y de la empresa de la que dependerá la Autoridad de Registro.

Cada incorporación de una nueva Autoridad de Registro Delegada se incluirá en el listado disponible en el sitio web del certificador con sus datos de contacto y nombre de su responsable.

Cada Autoridad de Registro Delegada estará integrada por los siguientes roles:

Responsable de la AR: es el responsable ante el certificador licenciado del funcionamiento de la Autoridad de Registro Delegada y del cumplimiento de los términos establecidos en el contrato correspondiente. Puede ser a su vez un oficial de Registro.

Oficial de Registro: se designarán oficiales de registro, quienes tendrán a su cargo la operatoria de aprobación y demás trámites relacionados con las solicitudes de certificados que se presenten ante la Autoridad de Registro.

Suscriptores de certificados.

Los procedimientos descriptos en el presente manual, en sus partes pertinentes a cada clase de certificado, son de aplicación obligatoria para los solicitantes y suscriptores de certificados.

Según los términos de la presente Política Única de Certificación, se define la Comunidad de Suscriptores de certificados digitales a todas las Personas Físicas o Jurídicas de naturaleza Pública o Privada o responsables autorizados de aplicaciones y sitios seguros, que suscriban certificados de firma digital o provisión de alguno o todos los servicios vinculados de firma digital con **LAKAUT S.A.**

Terceros Usuarios.

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 a la normativa vigente. En el caso de los certificados de sitio seguro, serán Terceros Usuarios quienes verifiquen el certificado del servidor.

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.

Administración de la Política.

Responsable del Documento.

LAKAUT S.A. es el responsable del mantenimiento e interpretación del Manual de Procedimientos de la Política Única de Certificación.

Contacto: El responsable de la Autoridad de Registro Central de la **AC – LAKAUT.**
Domicilio: Lima Nº 355. C1073AAG. Buenos Aires

Correo electrónico: info@lakautac.com.ar

Teléfono: +54 11 4382 4193/2856

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

Contacto.

LAKAUT S.A. es el responsable del registro, mantenimiento e interpretación del Manual de Procedimientos de la Política Única de Certificación.
Contacto: El responsable de la Autoridad de Registro Central de la **AC – LAKAUT.**
Domicilio: Lima Nº 355. C1073AAG. Buenos Aires

Correo electrónico: info@lakautac.com.ar

Teléfono: +54 11 4382 4193/2856

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

Procedimiento de aprobación de la Política Única de Certificación.

Conforme a lo establecido por el artículo 21 inc. q) de la Ley de Firma Digital Nº 25.506 y por el artículo 55 de la Decisión Administrativa Nº 927 del 30 de octubre de 2014, emitido el dictamen legal y técnico que acredite la aptitud del certificador, el ente licenciante procederá al dictado del acto administrativo correspondiente, otorgando la respectiva licencia y ordenando su publicación en el BOLETÍN OFICIAL DE LA REPÚBLICA ARENTINA.

Definiciones y Acrónimos.

Definiciones.

Se incluirán las definiciones de los conceptos relevantes utilizados en la Política de Certificación, incluyendo los siguientes:

- **Autoridad de Aplicación:** la SECRETARÍA DE GABINETE Y COORDINACIÓN ADMINISTRATIVA de la JEFATURA DE GABINETE DE MINISTROS es la Autoridad de Aplicación de firma digital en la REPÚBLICA ARGENTINA.
- **Autoridad de Registro**: es la entidad que tiene a su cargo las funciones de:

- Recepción de las solicitudes de emisión de certificados.
- Validación de la identidad y autenticación de los datos de los titulares de certificados.
- Validación de otros datos de los titulares de certificados que se presenten ante ella cuya verificación delegue el Certificador Licenciado **LAKAUT S.A.**
- Remisión de las solicitudes aprobadas al Certificador Licenciado **LAKAUT S.A.** con la que se encuentre operativamente vinculada.
- Recepción y validación de las solicitudes de revocación de certificados; y su direccionamiento al Certificador Licenciado **LAKAUT S.A.** 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 Única de Certificación y el Manual de Procedimientos del Certificador Licenciado con el que se encuentre vinculada, en la parte que resulte aplicable.

Dichas funciones son delegadas por el certificador licenciado. Puede actuar en una instalación fija o en modalidad móvil, siempre que medie autorización del ente licenciante.

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

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

- **Certificación digital de fecha y hora:** Indicación de la fecha y hora cierta, asignada a un documento o registro electrónico por una tercera parte confiable y firmada digitalmente por ella. (Anexo al Decreto N° 2628 de fecha 19 de diciembre de 2002).

- **Ente licenciante:** la SUBSECRETARÍA DE TECNOLOGÍAS DE GESTIÓN de la SECRETARÍA DE GABINETE Y COORDINACIÓN ADMINISTRATIVA de la JEFATURA DE GABINETE DE MINISTROS es Ente Licenciante.

- **Lista de certificados revocados:** Lista de certificados que han sido dejados sin efecto en forma permanente por el Certificador Licenciado, la cual ha sido firmada digitalmente y publicada por el mismo. En inglés: Certificate Revocation List (CRL). (Anexo al Decreto N° 2628/02)

- **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). (Anexo al Decreto N° 2628/02)

- **Plan de Cese de Actividades:** conjunto de actividades a desarrollar por el certificador licenciado en caso de finalizar la prestación de sus servicios. (Anexo al Decreto N° 2628/02)

- **Plan de Continuidad de las operaciones:** Conjunto de procedimientos a seguir por el certificador licenciado ante situaciones de ocurrencia no previstas que comprometan la continuidad de sus operaciones.

- **Plan de Seguridad:** Conjunto de políticas, prácticas y procedimientos destinados a la protección de los recursos del certificador licenciado. (Anexo al Decreto N° 2628/02).

- **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.

- **Servicio OCSP (Protocolo en línea del estado de un certificado – "Online Certificate Status Protocol"):** servicio de verificación en línea del estado de los certificados. El OCSP es un método para determinar el estado de revocación de un certificado digital usando otros medios que no sean el uso de Listas de Revocación de

Certificados (CRL). El resultado de una consulta a este servicio está firmado por el certificador que brinda el servicio.

- **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 física o jurídica que recibe un documento firmado digitalmente y que genera una consulta para verificar la validez del certificado digital correspondiente. (artículo 3° del Decreto N° 724/06).

Acrónimos.

CRL - Lista de Certificados Revocados (“Certificate Revocation List”)

CUIT - Clave Única de Identificación Tributaria.

IEC - International Electrotechnical Commission.

IETF - Internet Engineering Task Force .

OCSP - Protocolo en línea del estado de un certificado (“On line Certificate Status Protocol”).

OID - Identificador de Objeto (“Object Identifier”)

ONTI - Oficina Nacional de Tecnologías de Información.

RFC - Request for Comments.

RESPONSABILIDADES VINCULADAS A LA PUBLICACIÓN Y A LOS REPOSITORIOS.

Repositorios.

LAKAUT S.A. presta el servicio de repositorio conforme a lo establecido en el apartado 2.1.5 de la Política Única de Certificación y es quien presta directamente tal servicio.

Publicación de información del certificador.

El Certificador garantizará el acceso a la información actualizada y vigente publicada en el repositorio que mantiene en línea y de acceso público, de la siguiente documentación:

- **A.** Política Única de Certificación en sus versiones vigentes y anteriores
- **B.** El modelo del Acuerdo con Suscriptores.
- **C.** Política de Privacidad.
- **D.** Manual de Procedimientos en sus aspectos de carácter público, versiones vigentes y anteriores.
- **E.** Información relevante de los informes de su última auditoría.
- **F.** Los Términos y Condiciones con Terceros Usuarios (“relying parties”)
- **G.** La lista de certificados revocados (CRL).
- **H.** Repositorio de certificados revocados.
- **I.** Certificados del Certificador licenciado y acceso al de la Autoridad Certificante Raíz.
- **J.** Su certificado digital.
- **K.** Su certificado OCSP.

Frecuencia de publicación.

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

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.

La información antedicha se encuentra disponible durante las VEINTICUATRO (24) horas los SIETE (7) días de la semana en el sitio web del Certificador https://www.lakautac.com.ar y se actualiza inmediatamente después de revocarse un certificado o emitirse uno, y en ningún caso superará una demora de VEINTICUATRO (24) horas.

Independientemente de un suceso de revocación de un certificado, la lista de certificados revocados (CRL) se renueva cada 24 horas aunque no tuviere modificaciones.

Las actualizaciones al resto de la información contenida en el repositorio, se realizarán en un plazo menor a VEINTICUATRO (24) horas.

Controles de acceso a la información.

Se garantizan los controles de los accesos al certificado del certificador, a la Lista de Certificados Revocados y a las versiones anteriores y actualizadas de la Política Única 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 por autoridad competente en el ámbito de los procedimientos administrativos.

En virtud de la Ley de Protección de Datos Personales N° 25.326 y a lo dispuesto por el inciso h) del artículo 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.

LAKAUT S.A. garantiza el acceso permanente, irrestricto y gratuito a la información publicada en su repositorio por parte de los suscriptores y terceros y es monitoreado permanentemente por medio de un centro de control con guardia permanente, que detecta la indisponibilidad o falla del servicio de certificación, reportando el incidente al personal que en ese momento está consignado como guardia específica para la AC – LAKAUT.

El personal se encuentra preparado para actuar inmediatamente y resolver a la brevedad el inconveniente. En caso de resultar infructuoso en un tiempo acorde a la gravedad de la falla, se aplicará el Plan de Contingencias que corresponda al evento en trato.

IDENTIFICACIÓN Y AUTENTICACIÓN.

La AC – LAKAUT emite certificados digitales a quienes cumplan con los requisitos para ser suscriptor, efectuándose una validación personal de la identidad del solicitante, para lo cual se requiere su presencia física ante la Autoridad de Registro.

El solicitante debe probar su carácter de suscriptor para la correspondiente Política Única de Certificación. La única excepción a la emisión de certificados para persona físicas es el caso del Certificado OCSP.

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

a) El solicitante ingresa al sitio web del Certificador https://www.lakautac.com.ar

b) Completa la solicitud de certificado con sus datos personales.

c) Acepta el Acuerdo con Suscriptores en el que se hace referencia a la Política que respalda la emisión del certificado.

d) Envía su solicitud a la **AC- LAKAUT** e imprime la Nota de Solicitud.

e) Verifica que el Código de Solicitud de la Nota de Solicitud coincida con el que aparece en la pantalla y en ese caso firma la Nota de Solicitud.

f) Se presenta ante la Autoridad de Registro correspondiente con la documentación requerida con el fin de realizar su identificación personal.

El Oficial de Registro efectúa los siguientes procedimientos con el fin de realizar la identificación del solicitante y corroborar la titularidad de la solicitud de certificado:

a) Verifica la existencia en el sistema de la solicitud

b) Al momento de presentación del solicitante o suscriptor en sus oficinas, valida su identidad mediante la verificación de la documentación requerida

c) Requiere al solicitante la firma de la nota de solicitud en su presencia

d) Resguarda toda la documentación respaldatoria del proceso de validación de la identidad de los solicitantes y suscriptores de certificados, luego de digitalizarla y a ambas las guarda por el término de DIEZ (10) años a partir de la fecha de vencimiento o revocación del certificado.

Cumplido el proceso de autenticación de su identidad, el solicitante firma la Nota de Solicitud de su certificado ante el Oficial de Registro de la Autoridad de Registro correspondiente, con lo cual acepta las condiciones de emisión y uso del certificado.

El Certificador se obliga a cumplir con las disposiciones de la Política Única de Certificación, con el Manual de Procedimientos vinculado a la misma, con las cláusulas del Acuerdo con Suscriptores y con la normativa aplicable a firma digital.

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

Asignación de nombres de suscriptores.

Tipos de nombres.

Los tipos de nombres se encuentran contenidos en el apartado 3.1. “Asignación de nombres de suscriptores de la Política Única de Certificación” de **LAKAUT S.A.**

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

Necesidad de Nombres Distintivos.

Los atributos mínimos incluidos en los certificados con el fin de identificar unívocamente a su titular se encuentran definidos en el apartado 3.1.2. de la Política Única de Certificación de **LAKAUT S.A.**

Se describen las denominaciones según el tipo de certificado que se emita: para los certificados de los proveedores de servicios de firma digital o de aplicación, para los certificados de Personas físicas, para los certificados de Personas jurídicas Públicas o Privadas o para los certificados de sitio seguro.

Anonimato o uso de seudónimos.

No se emitirán certificados anónimos o cuyo Nombre Distintivo contenga UN (1) seudónimo o nombre de fantasia.

Reglas para la interpretación de nombres.

El procedimiento de interpretación de nombres está implementado en la **AC – LAKAUT**, por medio de las rutinas adecuadas y desarrolladas al respecto. Las ambigüedades o conflictos que pudieran generarse cuando se usan caracteres especiales en los contenidos de los campos de información de certificados digitales se tratarán de modo de asegurar la compatibilidad de los datos almacenados en el certificado.

Respecto de la interpretación de ciertos caracteres especiales que pudieran estar presentes en el nombre o apellido del solicitante/suscriptor, éste último deberá reflejarlos de manera acorde a como están escritos en su documento de identificación personal.

Unicidad de nombres.

El nombre distintivo es único para cada suscriptor y está integrado por los campos indicados en el punto 3.1.2.

Reconocimiento, autenticación y rol de las marcas registradas.

No se permite el uso de marcas comerciales, marcas de servicios o nombres de fantasía como nombres distintivos en los certificados de la **AC – LAKAUT**, excepto en el caso de Personas Jurídicas o aplicaciones, en los que se aceptará en base a la documentación presentada por el solicitante.

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 el certificador o ante la Autoridad de Registro operativamente vinculada. Se establecen los medios admitidos para recibir los requerimientos de certificados y para comunicar su aceptación.

El certificador debe cumplir con la normativa descripta en el apartado 3.2.- de la Política Única de Certificación de LAKAUT S.A.

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 todos los aspectos regulados en el apartado 3.2.2 de la Política Única de Certificación de LAKAUT S.A.

Para la solicitud de un certificado de Persona Jurídica Pública o Privada, su representante legal, apoderado, administrador o autoridad competente, según el caso, completa la solicitud de certificado.

A continuación, se presenta ante la Autoridad de Registro Central o Delegada que corresponda con la siguiente documentación:

a) Documento de identidad (original y fotocopia). De tratarse de argentinos nativos o naturalizados, deberá presentar documento nacional de identidad, libreta cívica o libreta de enrolamiento. Los extranjeros deberán presentar documento nacional de identidad, de poseerlo, o bien pasaporte o documento de identidad del país de origen, cuando fuera aplicable, o certificado o comprobante que acredite el número de expediente asignado por la Dirección Nacional de Migraciones, donde conste el carácter de su residencia.

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.

- 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 documento que acredite la representación invocada y su documento de identidad.

c) Constancia de inscripción en el Registro Público de Comercio.

d) Constancia de inscripción en la Administración Federal de Ingresos Públicos (AFIP).

e) Documento Nacional de Identidad de todos los socios, en caso de sociedades irregulares.

f) Acta de distribución de cargos.

g) Poder General Amplio o Poder Especial que autoriza la solicitud de certificado de firma digital.

- 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.

El Oficial de Registro verificará la identidad de la persona que se presenta, comprobando asimismo su carácter de representante legal, apoderado, administrador o autoridad competente a través de la verificación de la documentación aportada.

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

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

Autenticación de la identidad de Personas Físicas.

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

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

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

2.- Extranjeros con residencia en el país -incluida la temporaria o transitoria- presentarán DNI, en caso de poseerlo. De no ser así, presentarán pasaporte o documento de identidad del país de origen, cuando fuera aplicable, o bien certificado o comprobante que acredite el número de expediente asignado por la Dirección Nacional de Migraciones, donde conste el carácter de su residencia.

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

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

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

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

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

Información no verificada del suscriptor.

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

Se indican a continuación los casos en que no se aprobará una solicitud de certificado digital.

a.- No es posible validar la identidad del solicitante:

Si la identidad del solicitante no ha podido ser validada satisfactoriamente por medio de los procedimientos indicados para el alta de un certificado digital, el Oficial de Registro no debe aprobar la solicitud y se debe realizar lo siguiente:

a. 1.- El Oficial de Registro debe informar al solicitante acerca de los elementos y/o pasos faltantes para finalizar satisfactoriamente el proceso de validación de su identidad.

a. 2.- El solicitante tiene un plazo de TREINTA (30) días corridos a partir de la generación de la solicitud, para proveer la información faltante o complementaria que se le solicite.

a.3.- En caso de no completarse el trámite pasado dicho plazo, la solicitud será revocada automáticamente por el sistema de la **AC – LAKAUT** y el solicitante debe reiniciar el proceso de solicitud de emisión del certificado digital, efectuando un nuevo requerimiento.

b.- El dispositivo criptográfico provisto por el solicitante no está homologado

Si el dispositivo criptográfico provisto por el solicitante no está aprobado por la **AC – LAKAUT**, el Oficial de Registro no debe aprobar la solicitud y se debe realizar lo siguiente:

b. 1.- El Oficial de Registro debe informar al solicitante que no es posible aprobar su solicitud debido a que el dispositivo criptográfico que pretende utilizar no está aprobado por la **AC – LAKAUT**.

b. 2.- El solicitante tiene un plazo de TREINTA (30) días corridos a partir de la generación de la solicitud, para presentarse nuevamente ante la Autoridad de Registro con un dispositivo criptográfico homologado por la **AC – LAKAUT**, oportunidad en que deberá repetirse la verificación de identidad del solicitante.

b.3.- En caso de no completarse el trámite pasado dicho plazo, la solicitud será revocada automáticamente por el sistema de la **AC – LAKAUT** y el solicitante debe reiniciar el proceso de solicitud de emisión del certificado, efectuando un nuevo requerimiento.

c.- Rechazo de solicitud.

En caso que una solicitud no sea aprobada en alguna de sus instancias en el término de TREINTA (30) días corridos desde su generación, caducará en forma automática por la ejecución de reglas internas del aplicativo de la **AC – LAKAUT**. El solicitante deberá realizar una nueva solicitud.

Validación de autoridad.

Según lo dispuesto en el apartado 3.2.2., el certificador o la Autoridad de Registro con la que se encuentre vinculado, verifica la autorización de la Persona Física que actúa en nombre de la Persona Jurídica para gestionar el certificado correspondiente.

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.

Requerimiento de revocación.

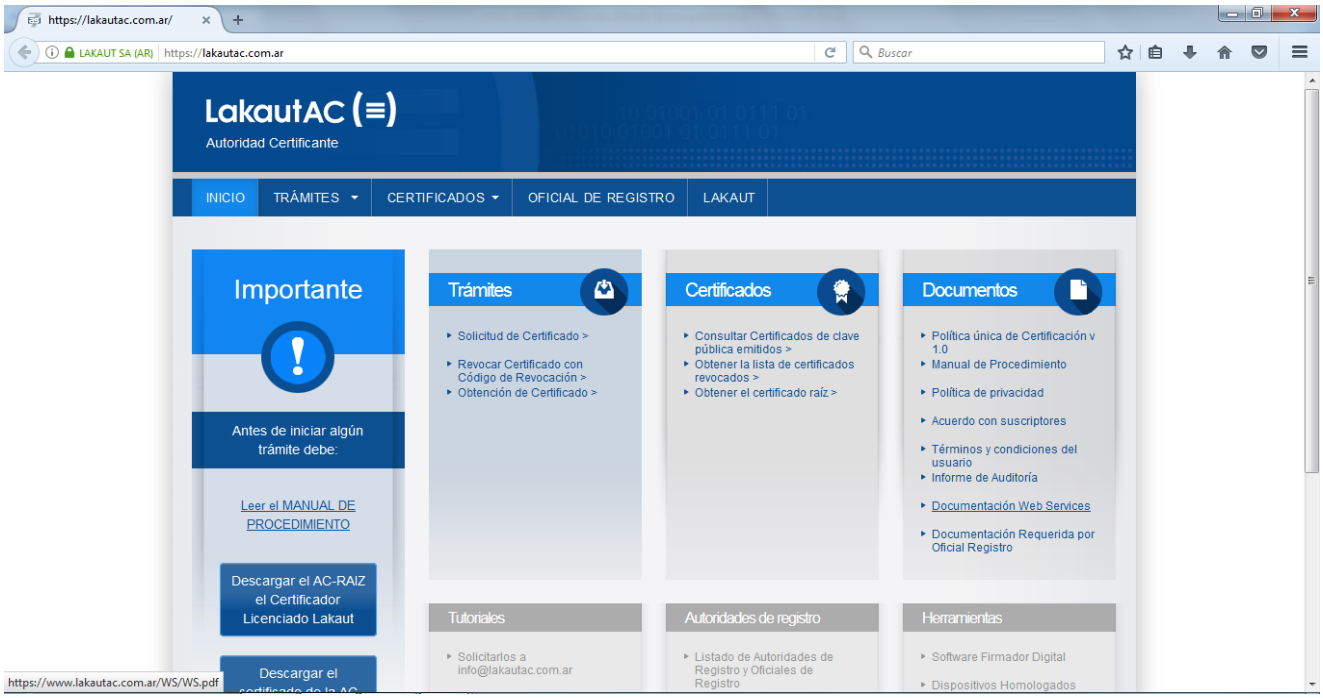
La **AC – LAKAUT** admite y procesa solicitudes de revocación recibidas de los suscriptores, en caso de personas físicas, o del representante legal de la organización, en caso de personas jurídicas, conforme a los procedimientos descriptos en el apartado 4.9 y siguientes del Formulario de Adhesión a la Política Única de Certificación de **LAKAUT S.A.** y los puntos 4.1.9.1 al 4-1.9.12 de la citada Política Única.

CICLO DEL CERTIFICADO: REQUERIMIENTOS OPERATIVOS.

Solicitud de certificado.

- El primer paso para obtener un Certificado Digital se realiza ingresando por la página web de Lakaut AC, www.lakautac.com.ar y dentro de ella en la barra de opciones Firma Digital.

Allí se presenta la página de inicio de Lakaut AC la cual despliega un menú de opciones.



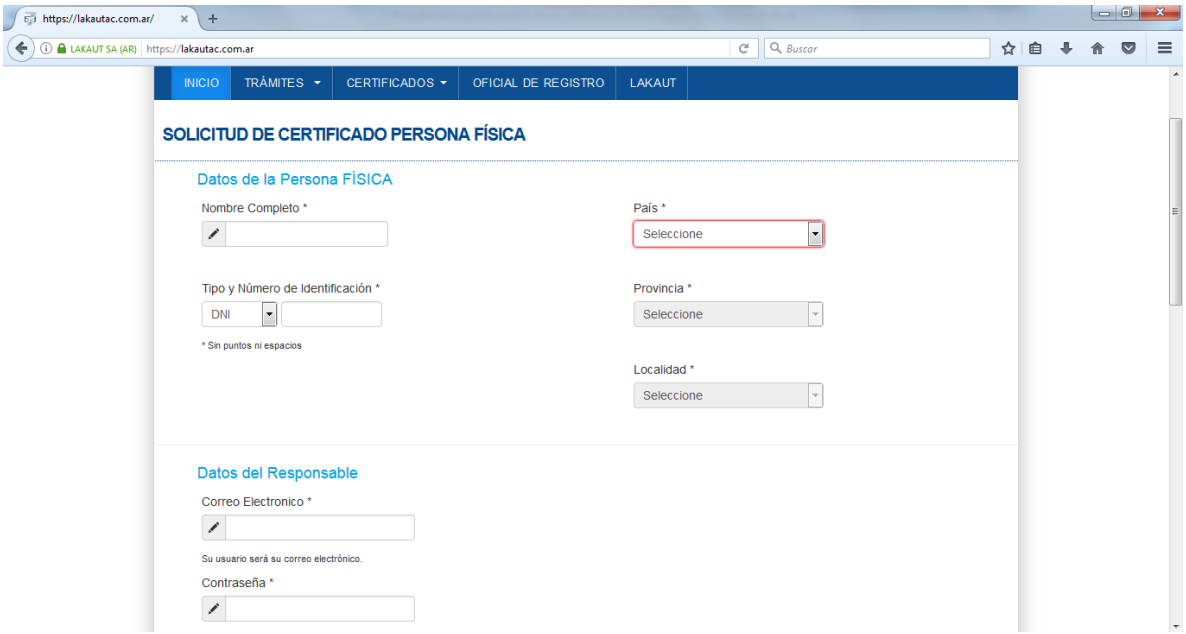
El primer paso sugerido consiste en que el suscriptor lea el manual de procedimientos a fin de interiorizarse de las distintas modalidades e implicancias de la obtención de un certificado de Firma Digital, así como descargar la AC raíz de Lakaut y el certificado Raíz de la República Argentina.

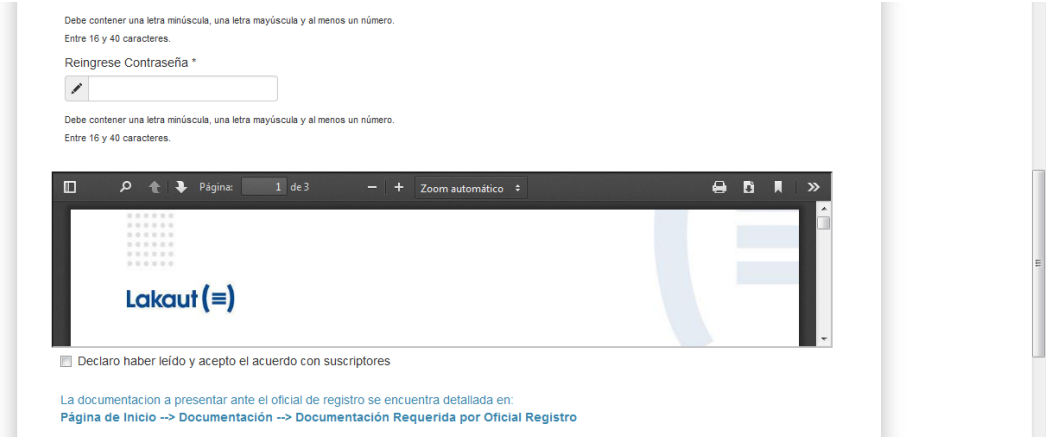
Posteriormente debe ingresar al siguiente punto del menú: “Solicitud de Certificado”, en la sección “Trámites” del sitio.

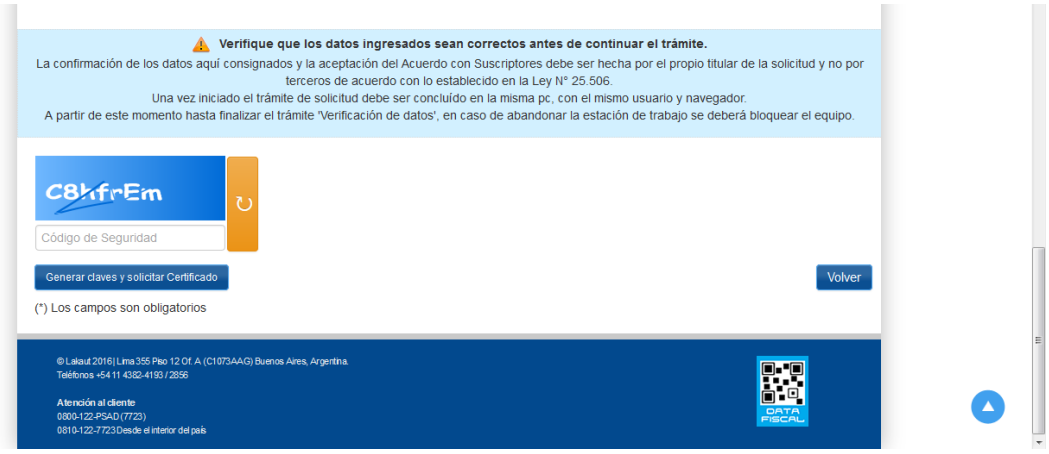
Aquí se le desplegará una ventana con los **"requisitos tecnológicos"** para proceder con la carga de la solicitud del Certificado y la **"Guía Paso a Paso"** que contiene instrucciones y las etapas que se deben tener en cuenta esencialmente, en el proceso de solicitud.

Como se puede visualizar, en la imagen que antecede, desde esa pantalla se puede acceder y elegir si se trata de una solicitud de Certificado para Persona Jurídica o para Persona Física.

Aclaración: Continuaremos el desarrollo del presente, seleccionando y usando como ejemplo “Persona Física”, señalando que el mecanismo es igual para los dos casos.

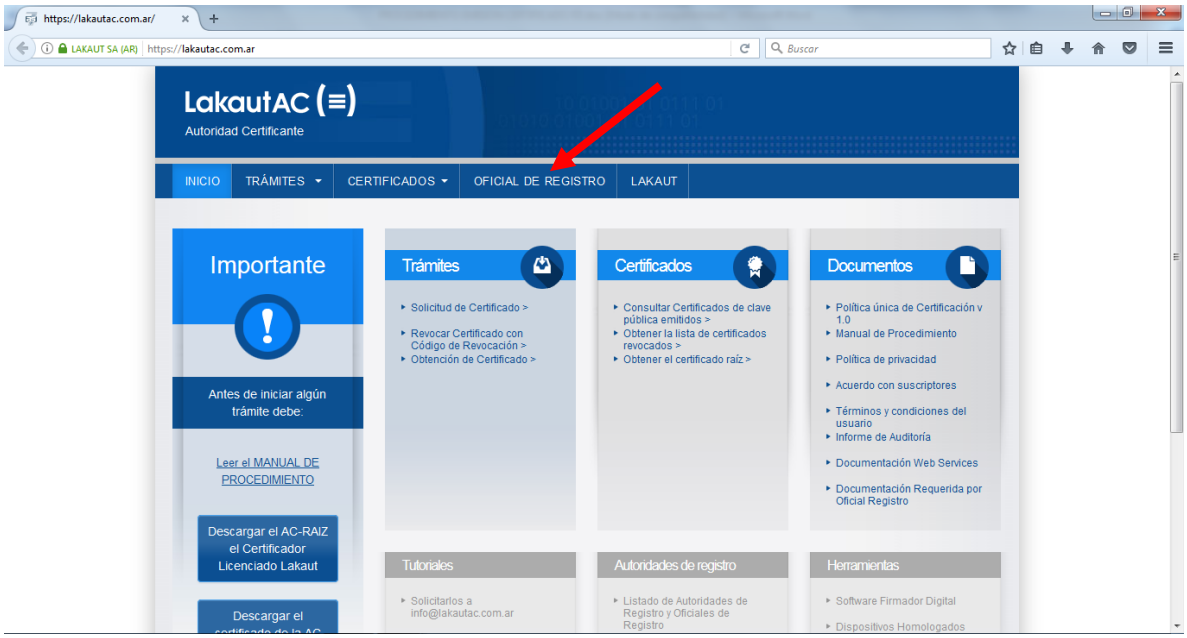






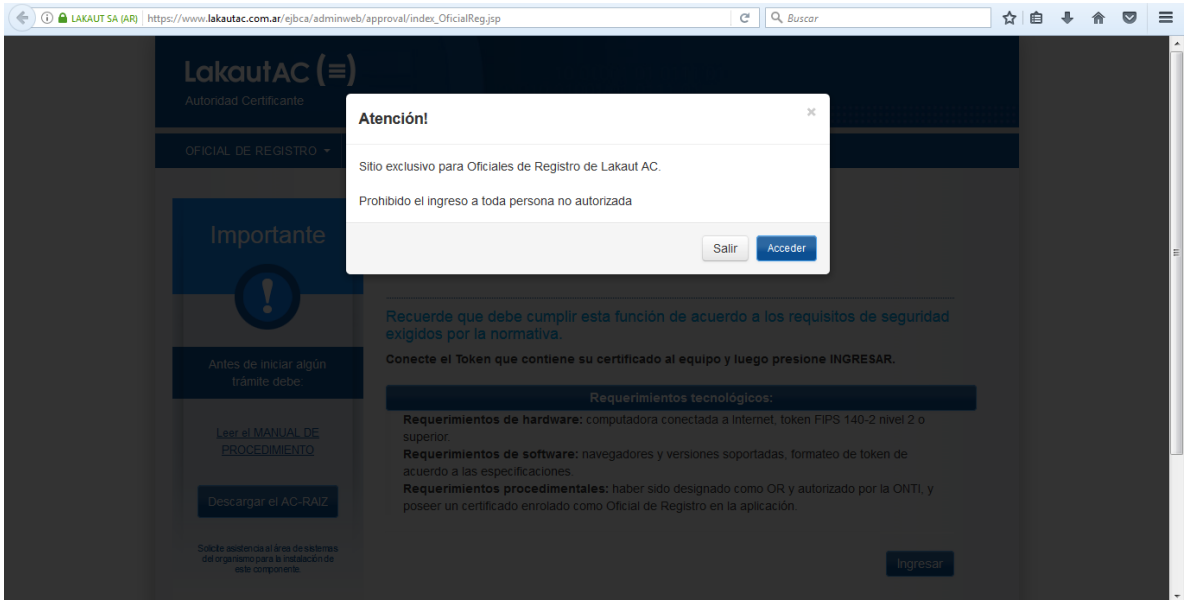
Completado por el solicitante todos y cada uno de los datos requeridos en el formulario de solicitud de Certificado, este tal cual se indica en la “Guía paso a paso”, debe ser impreso para luego ser presentado ante la Autoridad de Registro correspondiente, previa concertación del turno respectivo.

Concertado el turno y con el potencial suscriptor en presencia del Oficial de Registro, éste habiendo analizado la documentación respaldatoria (que queda en poder del Oficial de Registro) y acreditada la identidad del solicitante, debe ingresar al sistema de la aplicación de firma, desde el menú creado al efecto.

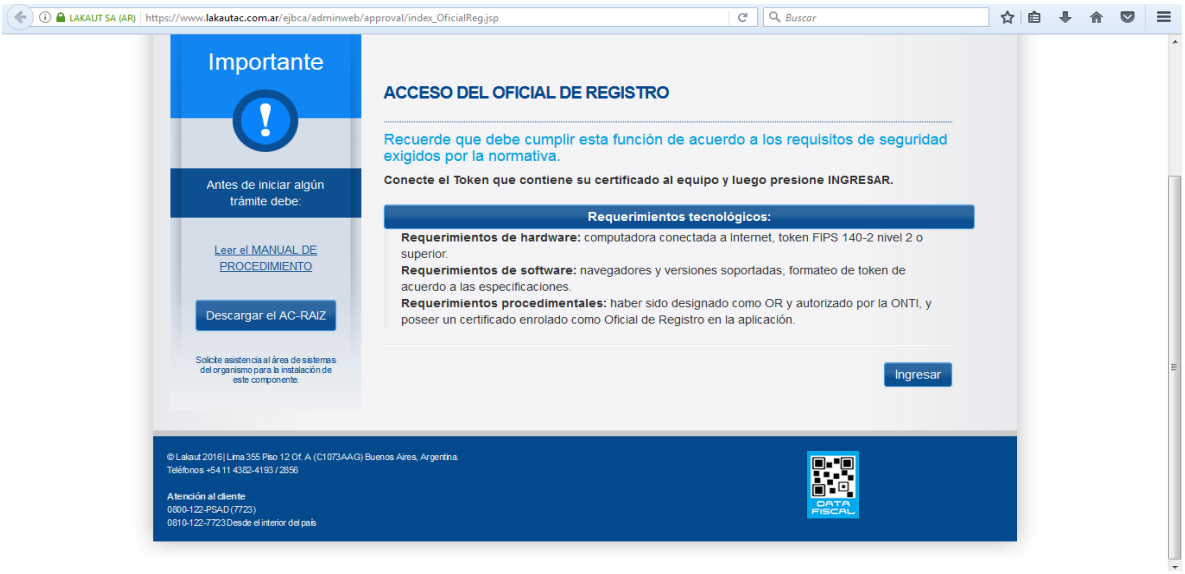


El Oficial de Registro ingresa al sistema con su dispositivo criptográfico (Token) que cumples con las exigencias legales correspondientes.

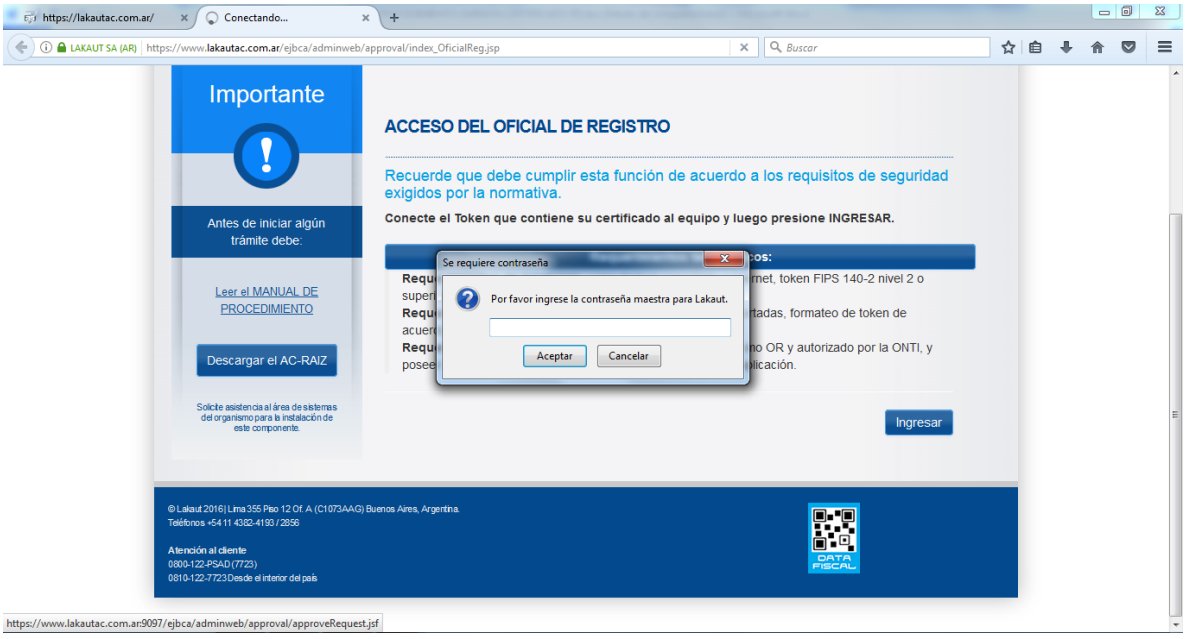
Al acceder se visualiza la advertencia de que esta sección es de uso exclusivo de las Autoridades de Registro de Lakaut AC.



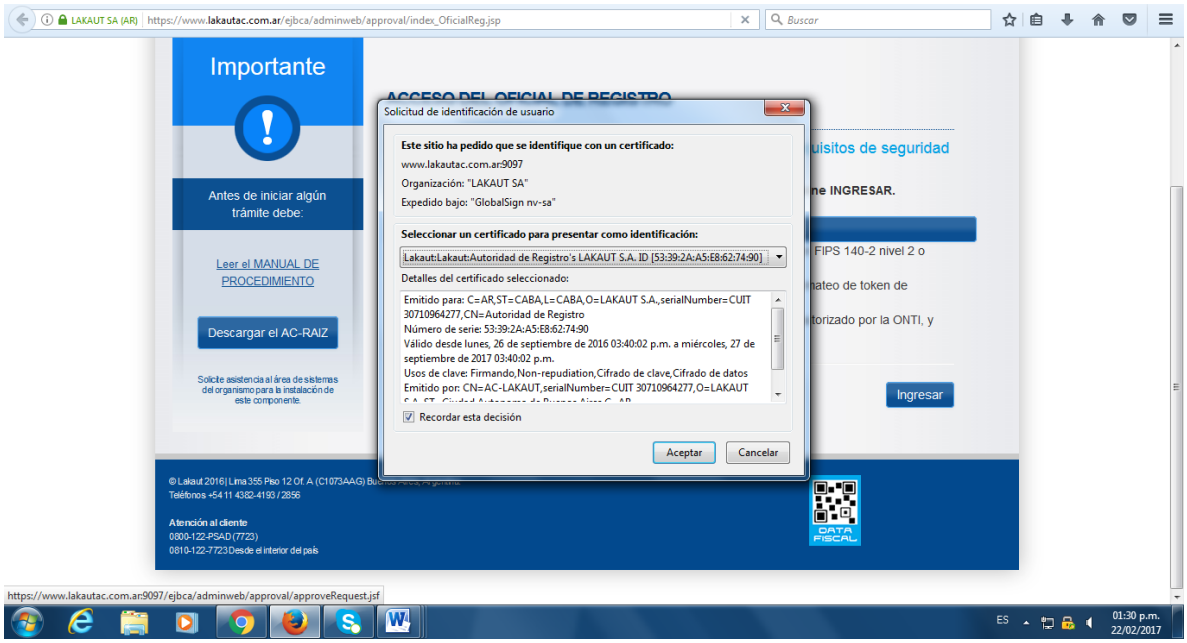
Acto seguido y dando clic en “Acceder”, se visualiza la siguiente pantalla, que recuerda el uso del Token respectivo y las condiciones tecnicas para la utilización del sistema, al Oficial de Registro.



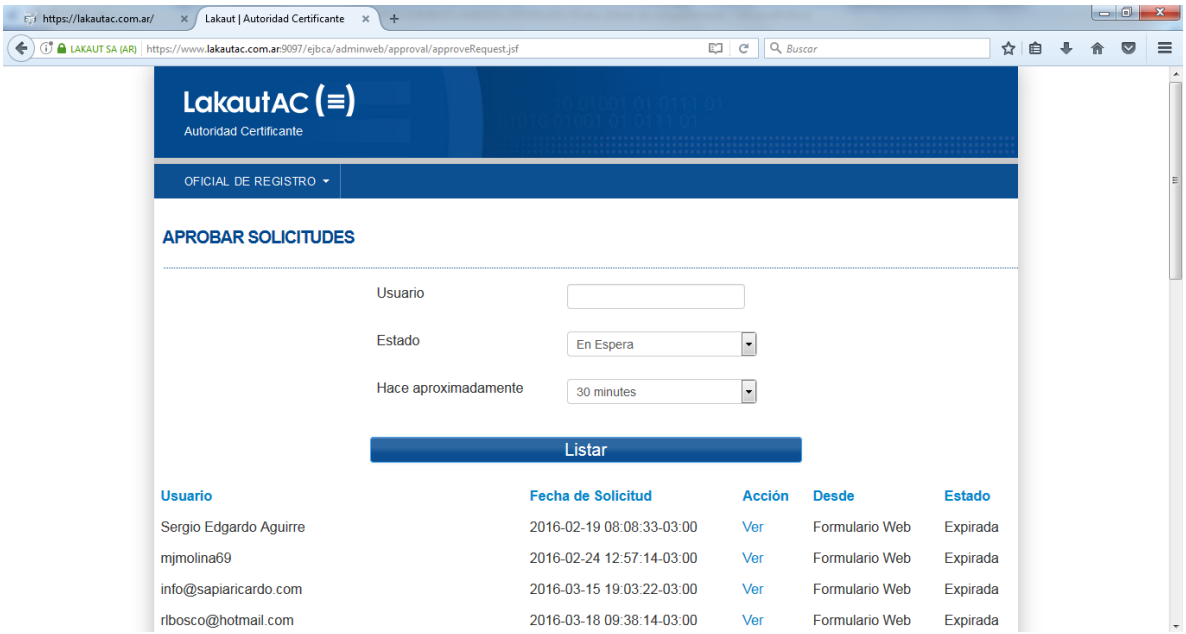
Damos clic en “Ingresar” y la aplicación solicitará la clave de ingreso para acceder al sistema.



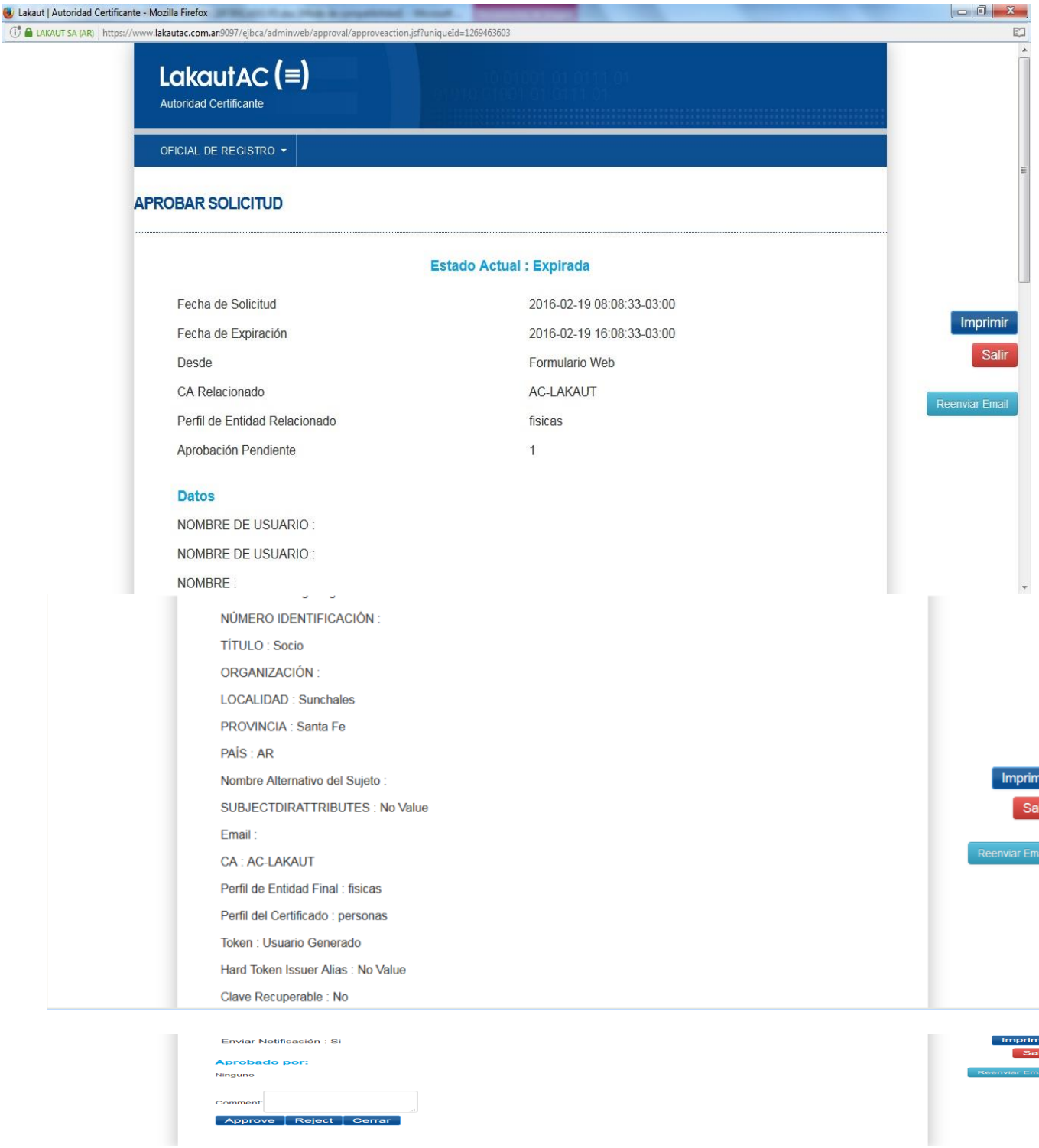
Se ingresa contraseña, de conocimiento exclusivo de la Autoridad de Registro en trato, y se da clic en “Aceptar”. Al hacerlo la aplicación muestra una ventana que refleja los datos de identificación del usuario que accede al sistema.



Se da clic en “Aceptar” y la aplicación ingresa a la lista de solicitudes registradas y cargadas en el sistema.



En esta pantalla el Oficial de Registro debe buscar y seleccionar la solicitud de que se trate. Elegida la misma, la aplicación lo lleva a la visualización de la solicitud y de los datos contenidos en ella. Al pie de la solicitud, se encuentran las opciones que tiene el Oficial de Registro, éstas son: Aprobarla, Recharzarla, o Cerrar la visualización, sin elegir ninguna de las anteriores, pudiendo volver a ingresar para culminar el proceso ya sea aprobando o rechazando la misma.



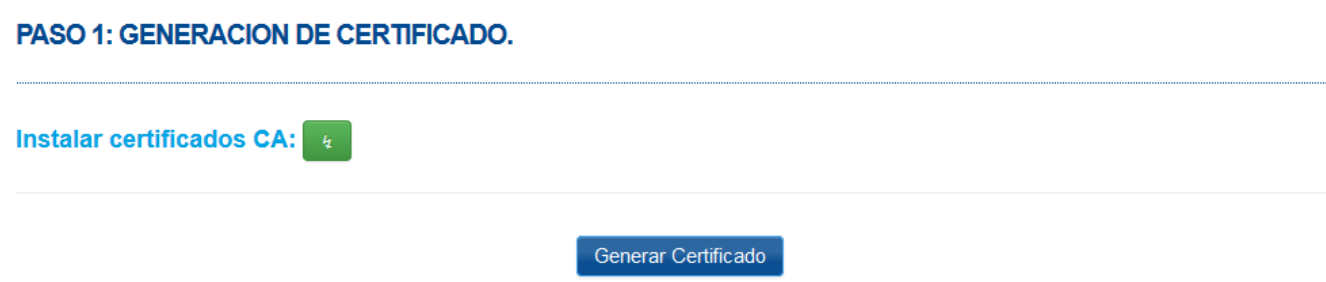
Para mejor visualizacion imagen ampliada de final de solicitud con opciones del Oficial de Registro.

Elegida una de las opciones, vamos a suponer que la solicitud queda aprobada, el sistema registra el evento de la aprobación y se visualiza de la siguiente forma. Lo mismo ocurre si la misma es rechazada, visualizandose tal acción.

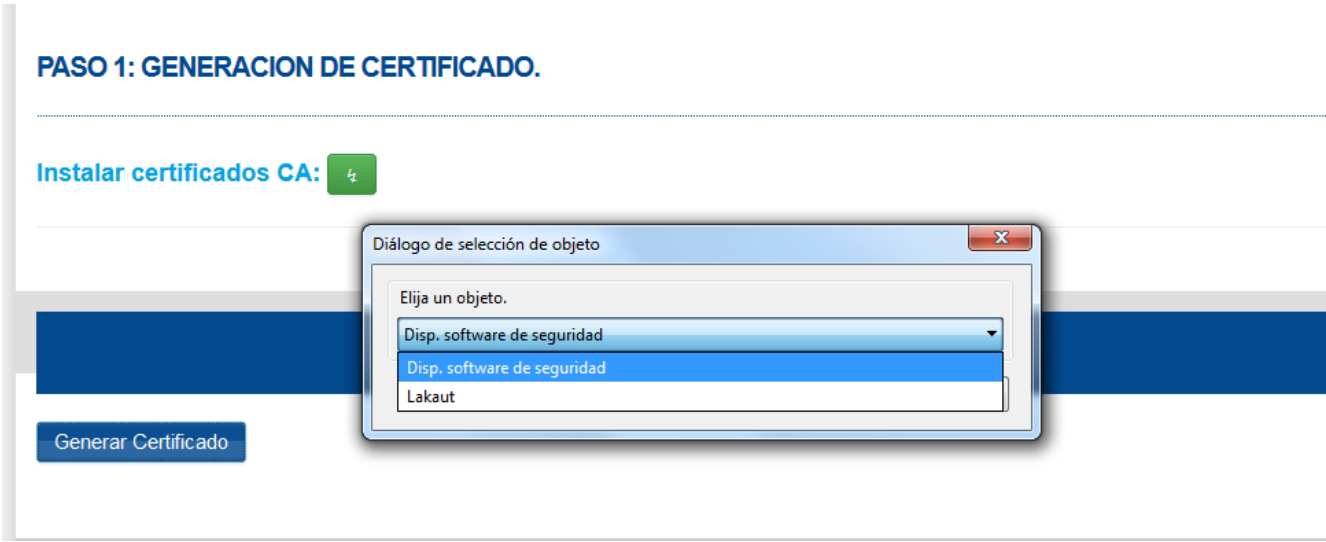
Una vez aprobada la solicitud el suscriptor debera ingresar, desde la pagina de lakautAC, a la opcion *Obtenciòn de Certificado.*

Luego se solicitara al suscriptor que ingrese el correo y la contraseña.

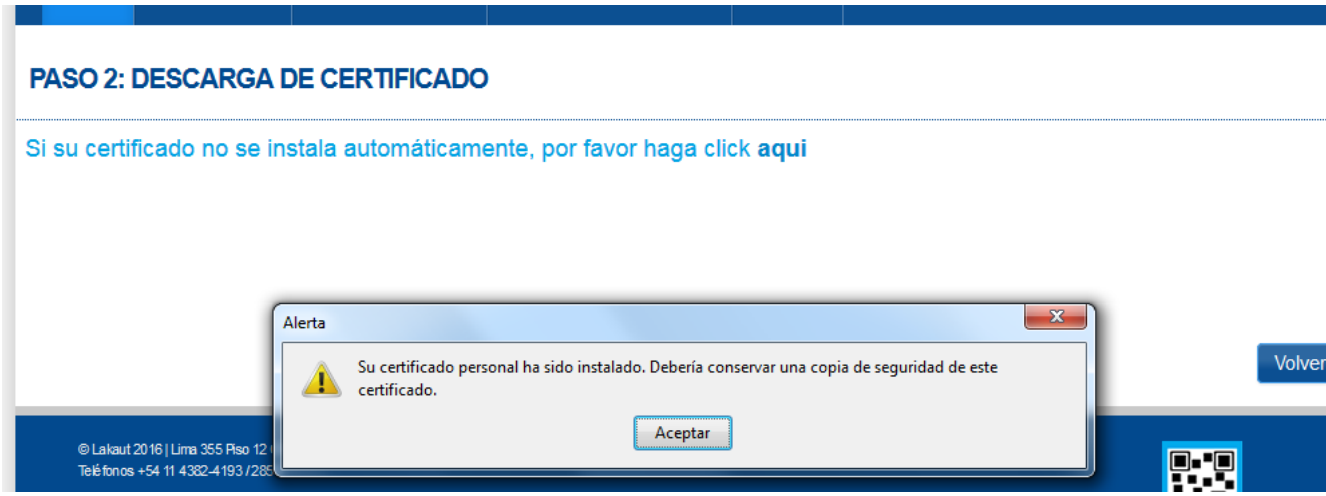
Una vez validado el mail y la contraseña se mostrata la siguiente pantalla para descargar el certificado.



Con el boton generar Certificado se procede a mostrar la siguiente pantalla, donde el suscriptor debe seleccionar el repositorio(Dispositivo de seguridad) de destino(Hardware o Software(Disp. Software de Seguridad))



Luego de seleccionar el repositorio y apretar el boton aceptar se instalara el certificado, apareciendo la siguiente pantalla.



Emitido el certificado y una vez recibido por el usuario/suscriptor, éste previo a la habilitación del uso del Certificado, deberá firmar ante la Autoridad de Registro el Acuerdo de Suscriptores correspondiente.

Aceptación del certificado.

Un certificado emitido a favor de un suscriptor se considera aceptado por su titular una vez que el suscriptor firmó el Acuerdo con Suscriptores y que el certificado haya sido puesto a su disposición.

Si el solicitante no acepta explícitamente y/o no retira su certificado digital dentro de los TREINTA (30) días corridos desde su emisión, se procederá a su revocación en forma automática.

Usos del par de claves y del certificado.

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

El suscriptor de un certificado digital deberá resguardar y no divulgar el uso de la clave privada y de su certificado a lo dispuesto por el apartado 4.5. de la Política Única de Certificación de **LAKAUT S.A.**

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.

Renovación del certificado.

En el caso de certificados digitales de Personas Físicas, 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 Físicas.

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.

Modificación del certificado.

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

.

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.

Causas de Revocación.

El Certificador 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 (Nota para el certificador: se deberá indicar lo que corresponda).
- 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 Resolución de la Autoridad de Aplicación.
- 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, del Decreto Reglamentario N° 2628/02 y demás normativa sobre firma digital.
- Por revocación de su propio certificado digital.

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

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

Autorizados a solicitar la revocación.

Se encuentran autorizados a solicitar la revocación de UN (1) certificado emitido por el certificador:

a) El suscriptor del certificado.
b) El responsable autorizado que efectuara el requerimiento, en el caso de certificados de persona jurídica o de aplicación.
c) El responsable autorizado por la Persona Jurídica que brinda el servicio o es titular del certificado o la aplicación, en el caso de los certificados de aplicación.
d) El responsable autorizado por la Persona Jurídica responsable del sitio web, en el caso de certificados de sitio seguro.
e) Aquellas personas habilitadas por el suscriptor del certificado a tal fin, previa acreditación fehaciente de tal autorización.
f) El certificador o la Autoridad de registro operativamente vinculada.
g) El ente licenciante.
h) La autoridad judicial competente.
i) La Autoridad de Aplicación.

Procedimientos para la solicitud de revocación.

El titular de un certificado digital emitido por la **AC – LAKAUT**, puede solicitar la revocación de un certificado digital del cual es suscriptor, mediante alguno de los siguientes procedimientos:

- Por presentación personal ante cualquier Autoridad de Registro de la **AC – LAKAUT**.

- Sin requerimiento del suscriptor, a través del sitio web de Lakaut AC.

La **AC – LAKAUT**, sin requerimiento del suscriptor, puede determinar la revocación del certificado si detecta algún caso previsto en la Ley Nº 25.506, artículo 19 inc. e), o en el Decreto Nº 2628/02, artículo 23.

Revocación a solicitud del titular del certificado digital.

Los titulares de certificado, en caso de Personas Físicas, o del representante legal de la organización, en caso de Personas Jurídicas, pueden solicitar la revocación de un certificado digital mediante alguno de los siguientes procedimientos:

Por medio del código de revocación.

Utilizando su código de revocación alfanumérico unívoco obtenido al efectuar la solicitud del certificado e ingresando al sitio web: (http://lakautac.com.ar) y selecciona la opción “Revocar”.

A continuación, elige una de las siguientes opciones:

a) Se autentica con su certificado digital.

b) Ingresa con el código alfanumérico unívoco que le fue suministrado al momento de efectuar su solicitud y su número de documento de identidad.

c)Completa el campo Motivo (obligatorio) y el detalle (optativo).

d)Al presionar el botón “Revocar”, la aplicación solicita la reconfirmación de la revocación.

e)Confirma la solicitud de revocación de su certificado.

f)La aplicación solicita al sistema la revocación del certificado.

g)Actualiza el estado del certificado a “Certificado revocado”.

h)La aplicación avisa a través de un correo electrónico al suscriptor que su certificado ha sido revocado.

Personalmente ante una Autoridad de Registro de la AC – LAKAUT.

El solicitante deberá presentarse personalmente ante una Autoridad de Registro de la **AC – LAKAUT** dentro de los horarios de atención, con documento de identidad y deberá manifestar al Oficial de Registro las causas de la solicitud de revocación e identificar el certificado que desea revocar.

El Oficial de Registro deberá verificar la identidad del solicitante, comprobando que el documento presentado coincida con el que figura en los registros de la Autoridad de Registro. De ser positiva la verificación, el Oficial de Registro ejecutará la opción de "Revocación de Certificado Digital" del Sistema Informático de la **AC – LAKAUT**, con los datos que le fueron suministrados en los pasos anteriores, y firmar digitalmente la operación con su propio dispositivo criptográfico.

De tratarse de representante legal, apoderado, administrador o autoridad competente, deberá presentar además documentación que acredite tal carácter.

Revocación por parte de la AC – LAKAUT.

Al detectarse la presencia de algún causal de revocación por parte de la AC – LAKAUT según la legislación vigente, el Responsable de la Autoridad de Registro revocará el o los certificados digitales que corresponda/n.

El Responsable de la Autoridad de Registro debe constatar que la causa de la revocación del certificado digital en cuestión esté dentro de las previstas por la política correspondiente al presente manual.

Debe ejecutar la opción "Revocación de Certificado Digital " del Sistema Informático de la **AC – LAKAUT**, con los datos del titular y del certificado digital en cuestión, colocar su causa y deberá firmar la transacción con su dispositivo criptográfico.

El Sistema Informático de la **AC – LAKAUT** prevé medios para realizar revocaciones múltiples en caso de existir varios certificados digitales afectados por un mismo causal de revocación, para facilitar la tarea. Este tipo de revocaciones son realizadas por el Responsable de la Autoridad de Registro mediante el menú correspondiente y se aplica el mismo procedimiento que para el caso de un único certificado digital.

Plazo para la solicitud de revocación.

Las solicitudes de revocación se gestionan en forma inmediata cuando se presente alguna de las circunstancias previstas en el apartado 4.9.1 y se hayan cumplido los procedimientos previstos en el apartado 4.9.3.

LAKAUT S.A. dispone de un servicio de recepción de solicitudes de revocación que se encuentra disponible en forma permanente SIETE (7) x VEINTICUATRO (24) horas a través de su aplicación web.

El plazo máximo entre la revocación y la publicación del estado del certificado, indicando la revocación, es de VEINTICUATRO (24) horas.

Plazo para el procesamiento de la solicitud de revocación.

El plazo 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.

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.

La autenticidad y validez de las listas de certificados revocados también debe ser confirmada mediante la verificación de la firma digital del certificador que la emite y de su período de validez.

El certificador cumple con lo establecido en el artículo 34, inciso g) del Decreto Nº 2628/02 relativo al acceso al repositorio de certificados revocados y las obligaciones establecidas en la presente Decisión Administrativa y sus correspondientes Anexos.

Frecuencia de emisión de listas de certificados revocados.

El Certificador genera y publica una Lista de Certificados Revocados con una frecuencia diaria, cada VEINTICUATRO (24) hs., con listas complementarias (delta CRL) en modo horario.

Vigencia de la lista de certificados revocados.

La vigencia de cada lista de certificados revocados es de VEINTICUATRO (24) horas.
El Certificador posee un servicio en línea de revocación de certificados y de verificación de su estado. Ambos servicios se encuentran disponibles SIETE (7) x VEINTICUATRO (24) horas, sujetos a un razonable calendario de mantenimiento.

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

La verificación del estado de validez de un certificado podrá efectuarse por alguno de los siguientes métodos:

Mediante el acceso a la lista de certificados revocados disponible en el sitio http://www.lakautac.com.ar/crl

Mediante el servicio en línea de consulta sobre estado del certificado (OCSP) disponible en el sitio web http://www.lakautac.com.ar/ocsp

Ambos servicios se encuentran disponibles SIETE (7) x VEINTICUATRO (24) horas, sujetos a un razonable calendario de mantenimiento. El Certificador garantiza el acceso permanente, eficiente y gratuito del público en general a ambos servicios.

Al momento de verificar una firma digital, con el fin de comprobar el estado de validez del certificado, los terceros usuarios deberán tener en cuenta que una vez que un certificado es revocado, esta circunstancia será reflejada en el servicio OCSP y en la próxima delta CRL a publicarse, en un plazo máximo de UNA (1) hora desde el momento de efectuada la revocación. Debido a esto con el fin de efectuar la correcta verificación del estado de validez de un certificado, los terceros usuarios deberán poseer la CRL correspondiente a las últimas VEINTICUATRO (24) hora.

Ante la falta de disponibilidad del sitio principal de publicación de la CRL, se cuenta con una instalación alternativa que responderá en forma inmediata a cualquier requerimiento de acceso y descarga de dicha lista, con idénticas prestaciones que el sitio principal.

Los certificados digitales emitidos por la **AC - LAKAUT** contienen la dirección de Internet de ambos puntos de distribución de la Lista de Certificados Revocados, como así también del servicio en línea de consulta sobre revocación de los certificados.

Requisitos para la verificación en línea del estado de revocación.

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

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

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

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

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

El uso del protocolo OCSP permite, mediante su consulta, determinar el estado de validez de un certificado digital y representa una alternativa a la consulta a la CRL, la que también estará disponible. El servicio OCSP se provee en el siguiente sitio web:

https://www.lakautac.com.ar/crt/lakaut.ocsp/

El servicio “OCSP responder” de la **AC- LAKAUT** devuelve los siguientes valores: “bueno" (good), "revocado" (revoked) o "desconocido" (unknown), para cada uno de los certificados para los que se ha efectuado una consulta.

Adicionalmente, como respuesta se puede devolver un código de error. Las respuestas se firman digitalmente con la clave privada correspondiente al certificado OCSP emitido bajo titularidad de la **AC – LAKAUT**, excepto en el caso del código de error antes referido.

Otras formas disponibles para la divulgación de la revocación.

El Certificador no utiliza otros medios para la divulgación del estado de revocación de los certificados que los contemplados en su Política de Certificación y cuyos procedimientos se encuentran descriptos en el presente Manual.

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.

El suscriptor del certificado es responsable de efectuar su revocación o bien de comunicar de inmediato de tal situación a la Autoridad de Registro cuando se den algunas de las siguientes causas:

a) Por compromiso o sospecha de compromiso de la clave privada.

b) Por pérdida de la clave privada.

c) Porque ya no sea posible su utilización.

d) Ante el conocimiento de que está ya no sea segura para operar.

e) Por cualquier otra circunstancia que el suscriptor considere que pueda resultar perjudicial a la seguridad de su clave privada.

LAKAUT S.A. operará en consecuencia a lo establecido en la Política Única de Certificación vinculada al presente Manual, procediendo a la revocación del certificado correspondiente y a notificar al suscriptor a través de un correo electrónico de dicha circunstancia. Asimismo procede a actualizar la CRL y la delta CRL correspondiente y a su publicación.

Causas de suspensión.

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

Autorizados a solicitar la suspensión.

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

Procedimientos para la solicitud de suspensión.

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

Límites del periodo de suspensión de un certificado.

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

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 del certificador.

De igual forma se producirá la desvinculación, ante el cese de las operaciones del certificador.

Recuperación y custodia de claves privadas.

El certificador licenciado no podrá bajo ninguna circunstancia realizar la recuperación o custodia de claves privadas de los titulares de certificados digitales, en virtud de lo dispuesto en el inciso b) del artículo 21 de la Ley N° 25.506. El suscriptor se encuentra obligado a mantener el control exclusivo de su clave privada, no compartirla e impedir su divulgación, de acuerdo a lo dispuesto en el inciso a) del artículo 25 de la ley antes mencionada.