POLÍTICA ÚNICA DE CERTIFICACIÓN
CERTIFICADOR LICENCIADO LAKAUT S.A.

Versión 2.0

ÍNDICE

1- INTRODUCCIÓN.

1.1.- Descripción general.

El presente documento establece las políticas que se aplican a la relación entre un Certificador Licenciado y los solicitantes, suscriptores y terceros usuarios de los certificados que éste emita en el marco de la Infraestructura de Firma Digital de la REPÚBLICA ARGENTINA (Ley N° 25.506 y normativa complementaria). Un certificado vincula los datos de una persona humana o jurídica o de una aplicación verificados por el Certificador Licenciado, convertidos a través de un procedimiento matemático, definido por la Secretaría de Innovación Pública como ente licenciante en una firma digital, que permiten identificar fehacientemente a dicho solicitante, conocido como suscriptor del certificado de manera Indubitable.

La presente Política Única de Certificación, Incluye el Identificador de Objeto (OID) correspondiente a esta política, otorgado por la Secretaría de Innovación Pública de la JEFATURA DE GABINETE DE MINISTROS o la que la reemplace en el futuro, quienes entienden en las funciones de Ente Licenciante.

1.2.- Nombre e Identificación del Documento.

a) Política Única de Certificación de LAKAUT S.A.

b) Versión: 2.0 Revisión: Cambios realizados según Decreto Reglamentario 182/2019 de la Ley de Firma Digital 25.506 y Resolución 946/2021 de la entonces Secretaría de Innovación Pública de la JEFATURA DE GABINETE DE MINISTROS.

c) Fecha de aplicación: A partir de su publicación en el Boletín Oficial de la República Argentina.

d) OID de la Política de Certificación: 2.16.32.1.1.5

e) Lugar o sitio de publicación: se publica en el sitio web de la **AC – LAKAUT www.lakautac.com.ar**

1.3.- Participantes

Integran la infraestructura del certificador las siguientes entidades:

1.3.1.- Certificador.

Razón Social: **LAKAUT S.A.**

Domicilio: Lima Nº 355. C1073AAG. Buenos Aires Teléfono: +54 11 4382 4193/2856
Correo electrónico: info@lakautac.com.ar CUIT: 30-7109642-7

1.3.2.- Autoridad de Registro.

Los datos de cualquiera de las Autoridades de Registro se publican en el siguiente sitio web: https://lakautac.com.ar/firma-digital/autoridadesDeRegistro

1.3.3.- Suscriptores de certificados.

Podrán ser suscriptores de los certificados emitidos por la Autoridad Certificante **AC - LAKAUT** las personas humanas o jurídicas sean éstas públicas o privadas, sin perjuicio de su posible ampliación previa notificación y aprobación por la Secretaría de Innovación Pública de la JEFATURA DE GABINETE DE MINISTROS.

La **AC - LAKAUT** será, además, suscriptora de un certificado para ser utilizado en relación con el servicio **On Line Certifícate Status Protocol** (en adelante, **OCSP)** de consulta sobre el estado de los certificados digitales.

1.3.4.- Terceros Usuarios.

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

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

1.4.- Uso de los certificados.

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

1.5.- Administración de la Política.

1.5.1.- Organización administradora del documento

Será responsable de la presente Política única de Certificación el máximo responsable del Certificador Licenciado de la Autoridad Certificante **LAKAUT.**

Correo electrónico: info@lakaut.com.ar

Teléfono: +54 11 4382 4193/2856

Domicilio: Lima Nº 355. C1073AAG. Buenos Aires

1.5.2.- Contacto.

Domicilio: Lima Nº 355. C1073AAG. Buenos Aires

Correo electrónico: autoridadderegistrocentral@lakautac.com.ar

Teléfono: +54 11 4382 4193/2856

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

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

La Política Única de Certificación se presenta ante la Secretaría de Innovación Pública de la JEFATURA DE GABINETE DE MINISTRO durante el proceso de renovación del licenciamiento para su aprobación dentro del correspondiente Acto Administrativo.

1.6 - Definiciones y Acrónimos

1.6.1 – Definiciones.

- **AUTORIDAD DE APLICACIÓN:** la Secretaría de Innovación Pública de la JEFATURA DE GABINETE DE MINISTROS responsable de firma digital en la REPÚBLICA ARGENTINA.
- **ACUERDO CON SUSCRIPTORES:** acuerdo entre Lakaut S.A. y el suscriptor determina los derechos y obligaciones de las partes en lo que respecta a la solicitud, aceptación y uso de certificados digitales.
- **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 la **AC – LAKAUT.**
- Remisión de las solicitudes aprobadas a **AC – LAKAUT** 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 de respaldo 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.
- Cumplimiento con la comprobación de la identidad del firmante, confronta mediante reconocimiento facial y datos biométricos de huella dactilar de los solicitantes y suscriptores de certificados de firma digital, utilizando el servicio de verificación de identidad provisto por el REGISTRO NACIONAL DE LAS PERSONAS o el que en el futuro lo reemplace

- **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 la Secretaría de Innovación Pública dependiente de la JEFATURA DE GABINETE DE MINISTRO como Autoridad de Aplicación de firma digital en la REPÚBLICA ARGENTINA. (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.

- **ENTE LICENCIANTE** la Secretaría de Innovación Pública dependiente de la JEFATURA DE GABINETE DE MINISTRO constituyen el Ente Licenciante.

- **LISTA DE CERTIFICADOS REVOCADOS:** Lista de certificados que han sido dejados sin efecto en forma permanente por el Certificador Licenciado, la cual ha sido firmada digitalmente y publicada por el mismo. En inglés: Certificate Revocation List (CRL).

- **MANUAL DE PROCEDIMIENTOS:** Conjunto de prácticas utilizadas por el certificador licenciado en la emisión y administración de los certificados. En inglés: Certification Practice Statement (CPS).

- **PLAN DE CESE DE ACTIVIDADES:** Conjunto de actividades a desarrollar por el certificador licenciado en caso de finalizar la prestación de sus servicios.

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

- **PLAN DE SEGURIDAD:** Conjunto de políticas, prácticas y procedimientos destinados a la protección de los recursos del certificador licenciado.

- **POLÍTICA DE PRIVACIDAD:** Conjunto de declaraciones que el Certificador Licenciado se compromete a cumplir de manera de resguardar los datos de los solicitantes y suscriptores de certificados digitales por él emitidos.

- **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 humana o jurídica que recibe un documento firmado digitalmente y que genera una consulta para verificar la validez del certificado digital correspondiente.
- **AUTORIDAD DE SELLO DE TIEMPO:**Entidad que acredita la fecha y hora cierta, asignada a un documento o registro electrónico por una tercera parte confiable y firmada digitalmente por ella.
- **AUTORIDAD DE SELLO DE COMPETENCIA:** Entidad que acredita competencias, roles, funciones o relaciones laborales del titular de un certificado de firma digital.

1.6.2 – Acrónimos.

CRL - Lista de Certificados Revocados (“Certificate Revocation List”) CUIT - Clave Única de Identificación Tributaria

OCSP - Protocolo en línea del estado de un certificado (“On line Certificate Status Protocol”)
OID - Identificador de Objeto (“Object Identifier”) RFC - Request for Comments
AC - LAKAUT - Autoridad Certificante de LAKAUT SA
AC - RAIZ – Autoridad Certificante Raíz de la REPÚBLICA Argentina
OR - Oficial de Registro
AR - Autoridad de Registro
OTP - One-Time Password

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

Se detallan a continuación las responsabilidades del AC-LAKAUT y de todo otro participante respecto al mantenimiento de repositorios, publicación de certificados y de información sobre sus políticas y procedimientos

Conforme a lo dispuesto por la Ley N° 25.506, la relación entre **AC - LAKAUT** y el titular de ese certificado se rige por el contrato que celebren entre ellos, sin perjuicio de las previsiones de la citada ley, y demás legislación vigente. Esa relación conforme el artículo 37 de la mencionada ley quedará encuadrada dentro del ámbito de responsabilidad civil contractual.

Al emitir un certificado digital o al reconocerlo en los términos del artículo 16 de la Ley 25.506, el

Certificador es responsable por los daños y perjuicios que provoque, por los incumplimientos a las previsiones de ésta, por los errores u omisiones que presenten los certificados digitales que expida, por no revocarlos, en legal tiempo y forma cuando así correspondiere y por las consecuencias imputables a la inobservancia de procedimientos de certificación exigibles todo ello de acuerdo con los establecido en el artículo 38 de la Ley N° 25.506. Corresponderá al Certificador demostrar que actuó con la debida diligencia.

El artículo 32, Capítulo IV del Decreto N° 182/2019, Reglamentario de la Ley N° 25.506, establece la responsabilidad del Certificador respecto de las AR.
En ese sentido prescribe que una AR puede constituirse como única unidad o con varias unidades dependientes jerárquicamente entre sí, pudiendo delegar su operatoria en otras AR, siempre que medie la aprobación del Certificador y este la obtenga del ente Licenciante previo a su habilitación.

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

El Certificador tampoco es responsable en los siguientes casos, según el artículo 39 de la Ley antes mencionada:

a) Por los casos que se excluyan taxativamente en las condiciones de emisión y utilización de sus certificados digitales y que no estén expresamente previstos en la Ley N° 25.506.
b) Por los daños y perjuicios que resulten del uso no autorizado de un certificado digital, si en las correspondientes condiciones de emisión y utilización de sus certificados constan las restricciones de su utilización;
c) Por eventuales inexactitudes en el certificado que resulten de la información facilitada por el titular que, según lo dispuesto en las normas y en los manuales de
procedimientos respectivos, deba ser objeto de verificación, siempre que el Certificador pueda demostrar que ha tomado todas las medidas razonables. Los criterios de valoración que seguirá la AR sobre la documentación aportada por el suscriptor para acreditar identidad u otros datos a incluir en el certificado, serán los normalmente aceptados en Derecho. La Autoridad de Registro siempre exigirá la presencia física del suscriptor en caso de nuevos certificados.

Todos los trámites realizados por las ARs son firmados digitalmente por los oficiales de registro y operadores que los realizan, asumiendo así su plena responsabilidad en el proceso.

Los alcances de la responsabilidad del Certificador se limitan a las consecuencias directas de la falta de cumplimiento de los procedimientos establecidos en esta Política Única de Certificación en relación a la emisión, renovación y revocación de certificados. Los alcances de la responsabilidad del Certificador se limitan a los ámbitos de su incumbencia directa, en ningún momento será responsable por el mal uso de los certificados que pudiera hacerse, tampoco por los daños y perjuicios derivados de la falta de consulta de la información disponible en Internet sobre la validez de los certificados, ni tampoco será responsable de los usos de los certificados en aplicaciones específicas.

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

2.1 – Repositorios.

Los repositorios de información y la publicación de la Lista de Certificados Revocados son administrados en forma directa por **LAKAUT S. A**., el servicio es propio y no es provisto por terceros.

2.2 – Publicación de Información del certificador.

El Certificador garantiza el acceso a la información actualizada y vigente publicada en el repositorio de los siguientes elementos:

a) Política Única de Certificación anterior y vigente.
b) Acuerdo con Suscriptores.
c) Términos y condiciones con Terceros Usuarios.
d) Política de Privacidad.
e) Manual de Procedimientos.
f) Información sobre las auditorías e inspecciones que le fueron efectuadas.
g) Repositorio de certificados revocados.
h) Certificados del Certificador Licenciado y acceso al de la Autoridad Certificante Raíz.

i) Consulta de certificados emitidos (indicando su estado).

2.3 – Listado de Autoridades de Registro - Frecuencia de publicación.

Se garantiza la actualización inmediata del repositorio cada vez que cualquiera de los documentos publicados sea modificado.
La Información antedicha se encuentra disponible en el sitio web del Certificador https://www.lakautac.com.ar
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.

2.4 – 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 de Certificación y a su Manual de Procedimientos.
Solo se revelará información confidencial o privada, si es requerida judicialmente o en el marco de 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, eficiente y gratuito de los titulares y terceros a la información publicada en su repositorio incluyendo la lista de certificados revocados y a disponer y dedicar los recursos necesarios para garantizar la seguridad de los datos almacenados, desde el punto de vista técnico y jurídico.

3.- IDENTIFICACIÓN Y AUTENTICACIÓN.

La AC – LAKAUT emite certificados digitales a quienes cumplan con los requisitos para ser suscriptor, efectuando 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.

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

a) El solicitante ingresa al sitio web del Certificador https://www.lakautac.com.ar/firma-digital/registracion?rauId=1

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** y la imprime.

e) Verifica que el Nro. de Solicitud coincida con el que aparece en la pantalla.

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) Cumple con la comprobación de la identidad del firmante, confrontando mediante reconocimiento facial y datos biométricos de huella dactilar de los solicitantes y suscriptores de certificados de firma digital, utilizando el servicio de verificación de identidad provisto por el REGISTRO NACIONAL DE LAS PERSONAS o el que en el futuro lo reemplace.

d) Requiere al solicitante la firma de la solicitud de certificado en su presencia

e) Firman la documentación: Solicitud, copia del DNI, Constancia de CUIL/CUIT del suscriptor, Acuerdo con Suscriptores y Acta labrada por el OR en libro de actas.

f) 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.

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.

Para la Renovación de Certificados se deberán cumplir los protocolos definidos en punto 3.3 y para la Revocación de Certificados en punto 3.4.

3.1– Asignación de nombres de suscriptores.

3.1.1– Tipos de Nombres.

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

3.1.2- Necesidad de Nombres Distintivos

Se indica las siguientes denominaciones, según el tipo de certificados que se emitan.

a. Para los Certificados de Aplicaciones:

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

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

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

- “serialNumbef (OID 2.5.4.5: Nro. de serie): Está presente y contiene el número de identificación de la Persona Jurídica Pública o Privada responsable del servicio o aplicación,

expresado como texto y respetando el siguiente formato y codificación: “[código de identificación]” “[nro. de identificación]”. El valor para el campo [código de identificación] es:

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

- “countryName” (OID 2.5.4.6: Código de país): Está presente y representa el país de emisión de los certificados, codificado según el estándar [IS03166] de DOS (2) caracteres.

b. Para los certificados de Personas humanas:

- “*commonName*” (OID 2.5.4.3: Nombre común): Está presente y se corresponde con el nombre que figura en el Documento de Identidad del suscriptor, acorde a lo establecido en el punto 3.2.3.
- “*serialNumber*” (OID 2.5.4.5: Nro. de serie): Está presente y contiene el tipo y número de identificación del titular, expresado como texto y respetando el siguiente formato y codificación: “[tipo de documento]” “[nro. de documento]”

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

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

c. Para los certificados de Personas Jurídicas Públicas o Privadas:

- “commonName” (OID 2.5.4.3: Nombre común): coincide con la denominación de la Persona Jurídica Pública o Privada o con el nombre de la unidad operativa responsable del servicio (ej. Gerencia de Compras).
- “organizationName” (OID 2.5.4.10: Nombre de la organización): Para certificados de aplicaciones, coincide con la denominación de la Persona Jurídica Pública o Privada.

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

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

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

d. Para los certificados de Sitio Seguro:

- “*commonName”* (OID 2.5.4.3: Nombre común): Contiene la denominación del sitio web de Internet que se busca proteger.
- “*organizationalUnitName*” (OID 2.5.4.11: Nombre de la Suborganización): Contiene a las unidades operativas de las que depende el sitio web, de corresponder, pudiendo utilizarse varias instancias de este atributo de ser necesario.
- “*organizationName*” (OID 2.5.4.10: Nombre de la Organización): Está presente y coincide con el nombre de la Persona Jurídica Pública o Privada responsable del sitio web.
- “*serialNumber*” (OID 2.5.4.5: Nro. de serie): Está presente y contiene el número de identificación de la Persona Jurídica Pública o Privada responsable del servicio o aplicación, expresado como texto y respetando el siguiente formato y codificación: “[código de identificación]” “[nro. de identificación]”.
El valor para el campo [código de identificación] es: “CUIT”: Clave Única de Identificación Tributaria para las Personas Jurídicas argentinas.
- “*countryName*” (OID 2.5.4.6: Código de país): Está presente y representar el país de emisión de los certificados, codificado según el estándar [ISO3166] de DOS (2) caracteres.

e. Para los Certificados de Autoridad de Sello de Tiempo.

- “commonName” (OID 2.5.4.3: Nombre común): Indica el nombre del servicio.
- “organizationName” (OID 2.5.4.10: Nombre de la organización): Coincide con la denominación de la Persona Jurídica Pública o Privada.

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

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

  b) “ID” [país]: Número de identificación tributaria para Personas Jurídicas extranjeras. El atributo [país] está codificado según el estándar [ISO 3166] de DOS (2) caracteres.

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

f. Para los Certificados de Autoridad de Sello de Competencia

- “commonName” (OID 2.5.4.3: Nombre común): Indica el nombre de la Autoridad de Competencia.
- “organizationName” (OID 2.5.4.10: Nombre de la organización): Coincide con la denominación de la Persona Jurídica Pública o Privada.
- “serialNumber” (OID 2.5.4.5: Nro de serie): Está presente y contiene el número de identificación de la Persona Jurídica Pública o Privada, expresado como texto y respetando el siguiente formato y codificación: “[código de identificación]” “[nro. de identificación]”. Los valores posibles para el campo [código de identificación] son: “CUIT”: Clave Única de Identificación Tributaria para las Personas Jurídicas argentinas.
- “countryName” (OID 2.5.4.6: Código de país): Está presente y representa el país de emisión de los certificados, codificado según el estándar [ISO 3166] de DOS (2) caracteres.

3.1.3 Anonimato o uso de seudónimos.

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

3.1.4 - Reglas para la interpretación de nombres.

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

3.1.5- Unicidad de nombres.

El nombre distintivo debe ser único para cada suscriptor, pudiendo existir más de un certificado con igual nombre distintivo si corresponde al mismo suscriptor. El procedimiento de resolución de homonimias se basa en la utilización del número de identificación laboral o tributaria, tanto en el caso de personas humanas como jurídicas.

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

No se admite la inclusión de marcas comerciales, marcas de servicios o nombres de fantasía como nombres distintivos en los certificados, excepto en el caso de personas jurídicas o aplicaciones, en los que se aceptará en base a la documentación presentada.
El certificador se reserva el derecho de tomar todas las decisiones referidas a posibles conflictos sobre la utilización y titularidad de cualquier nombre entre sus suscriptores conforme su normativa al respecto. En caso de conflicto, la parte que solicite el certificado debe demostrar su interés legítimo y su derecho a la utilización de un nombre en particular.

3.2 - Registro inicial.

Se describen los procedimientos a utilizar para autenticar, como paso previo a la emisión de UN (1) certificado, la identidad y demás atributos del solicitante que se presente ante 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.

LAKAUT AC cumple con lo establecido en los artículos 14, inciso b) y 21, inciso a) de la Ley de Firma Digital Nº 25.506, y normas complementarias.

3.2.1 - Métodos para comprobar la titularidad del par de claves

Se comprueba que el solicitante es el titular del par de claves mediante la verificación de la solicitud del certificado digital en formato PKCS#10, la cual no incluye la clave privada. Las claves siempre son generadas por el solicitante. En ningún caso el Certificador Licenciado ni sus Autoridades de Registro toman conocimiento, ni exigir o ni acceder bajo ninguna circunstancia a la clave privada de los solicitantes o titulares de los certificados, conforme el artículo 21 inciso b) de la Ley N° 25.506, y del artículo 21 inciso 3 del Anexo al Decreto Reglamentario N° 182/2019 y complementarias.

3.2.2 - Autenticación de la identidad de Personas Jurídicas Públicas o Privadas.

Se establece que la documentación requerida al solicitante de un certificado digital de Persona Jurídica es:

a. Documento de Identidad
- Argentinos nativos o naturalizados: original y fotocopia del documento nacional de identidad.
- Extranjeros con residencia en el país, presentarán DNI, en caso de poseerlo. De no ser así, presentarán pasaporte o documento de identidad del país de origen, cuando fuera aplicable.

b. Constancia de CUIL/CUIT del suscriptor, vigente.

c. Constancia de CUIT de la sociedad, vigente.

d. Copia certificada del instrumento que constituya la sociedad, según tipo societario.
- En caso de Personas Jurídicas Públicas, publicación en el boletín oficial de la constitución.

e. Copia certificada del instrumento que acredite el cargo dentro de la sociedad.
- En caso de Personas Jurídicas Públicas, publicación en el boletín oficial con designación de roles o autoridades.

f. En caso de apoderados no especiales. Nota con firma certificada del poderdante o miembro del directorio que autorice la obtención de la firma digital.

3.2.3 - Autenticación de la identidad de Personas Humanas.

La verificación de la identidad de los solicitantes de los certificados de personas Humanas se lleva de la misma manera que en el caso de Personas Jurídicas Públicas o Privadas con la única diferenciación de la documentación que se le solicita al potencial suscriptor, siendo en este caso, más sencilla. Se lleva a cabo mediante la constatación de los datos de número, apellidos, nombres y fotografía obrantes en el documento de identidad válido que el solicitante debe presentar ante el Oficial de Registro de la Autoridad de Registro. Luego el OR confrota la identidad del firmante, mediante reconocimiento facial y datos biométricos de huella dactilar de los solicitantes y suscriptores de certificados de firma digital, utilizando el servicio de verificación de identidad provisto por el REGISTRO NACIONAL DE LAS PERSONAS o el que en el futuro lo reemplace.

3.2.4 Información no verificada del suscriptor.

Se conserva la información referida al solicitante que no hubiera sido verificada. Adicionalmente, se cumple con lo establecido en el apartado 3 del inciso b) del artículo 14 de la Ley Nº 25.506. Se indican a continuación los casos en que no se aprobará una solicitud de certificado digital:

No es posible validar la identidad del solicitante:

a. 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:

- 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. 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.

- En caso de no completarse el trámite pasado dicho plazo, la solicitud expira 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.

c. El dispositivo criptográfico provisto por el solicitante no está homologado. Si el dispositivo criptográfico provisto por el solicitante “no cumple los requisitos de la PUC de la **AC – LAKAUT**, el Oficial de Registro no debe aprobar la solicitud y se debe realizar lo siguiente:

- 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**.

- 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**

d. En caso de contener un error debiendo rechazarla.

3.2.5 Validación de autoridad.

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

3.2.6 Criterios para la interoperabilidad.

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

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

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

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

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

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

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

En los casos a) y b) se exigirá el cumplimiento de los procedimientos previstos en el punto 3.4. - Autenticación de la identidad de Personas humanas.

Si la solicitud del nuevo certificado se realiza antes de la expiración del certificado, 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.

En los certificados de personas jurídicas o de aplicaciones, incluyendo los de servidores, se deberá tramitar UN (1) nuevo certificado, cumpliendo los pasos requeridos en el apartado 3.2.2. Autenticación de la identidad de Personas Jurídicas Públicas o Privadas.

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

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

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

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

3.4 Requerimiento de revocación

La **AC – LAKAUT** admite y procesa solicitudes de revocación recibidas de los suscriptores, en caso de personas Humanas, o del representante legal de la organización, en caso de personas jurídicas, conforme a los procedimientos descriptos en el apartado 3.4 del Manual de Procedimientos de **AC – LAKAUT.**

4 - CICLO DEL CERTIFICADO: REQUERIMIENTOS OPERATIVOS.

4.1 Solicitud de certificado.

Las solicitudes sólo podrán ser iniciadas por el solicitante en el caso de certificados de personas humanas y 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.

4.1.1 Solicitantes de certificados.

Los requerimientos técnicos con los que deberá contar el solicitante a fin de iniciar el proceso de solicitud se encuentran publicados en sitio web de la AC – LAKAUT. En caso de necesitar asistencia respecto de este tema o de los trámites que provee la AC – LAKAUT deberá contactarse con la mesa de ayuda de LAKAUT SA, donde un Analista de Atención al Cliente especializado en firma digital lo ayudará con el proceso. Los datos de contacto de los responsables se encuentran en el Listado de Autoridades de Registro y oficiales de registro publicado en el sitio web de la AC – LAKAUT.

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 humanas, 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 del Manual de Procedimientos de **AC – LAKAUT.**

Salvo que los Certificados a ser solicitados correspondan a Sitio Seguro o de Aplicación, al completar la solicitud el solicitante deberá seleccionar el nivel de seguridad del Certificado

Requerido (Alta seguridad).

4.1.2 - Solicitud de certificado

En primera instancia, es necesario 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.

4.2 Procesamiento de la solicitud del certificado.

La aprobación de los certificados para personas humanas, personas jurídicas, de sitio seguro o para aplicaciones está sujeta a que el solicitante cumpla con todos los requisitos solicitados para la obtención del certificado que solicita y a la verificación presencial de la identidad del solicitante. Cumplimiento con la comprobación de la identidad del firmante, confronta mediante reconocimiento facial y datos biométricos de huella dactilar de los solicitantes y suscriptores de certificados de firma digital, utilizando el servicio de verificación de identidad provisto por el REGISTRO NACIONAL DE LAS PERSONAS o el que en el futuro lo reemplace.

La autoridad de registro acredita la identidad del solicitante y verifica los datos de la solicitud pudiendo:

a. **Aprobar la solicitud**- Consiste en validar que los datos ingresados por el solicitante a la aplicación del Certificador sean coincidentes con la documentación que presenta al OR
Aprobados por el OR los datos ingresados al sistema de la AC, la aplicación del certificador al validar el requerimiento genera el PIN de revocación del certificado que se envía en un correo electrónico al solicitante, a la dirección de correo declarada por este en la solicitud. En el mismo correo se le comunica a su vez que su certificado se encuentra disponible para su descarga e instalación.
Con relación a la documentación acompañada por el solicitante al momento de presentarse ante el Oficial de Registro de la Autoridad de Registro Central o Delegada según sea el caso, esta deberá ser resguardada por el término de DIEZ (10) años a partir de la emisión del certificado o de su revocación.

b. **RECHAZO de la Solicitud**: Si la solicitud es rechazada, por errores en los datos

ingresados visualizados en la pantalla de solicitud, la solicitud es rechazada, previo explicarle las razones y los datos a corregir al solicitante por mail, quien en este caso deberá generar una nueva solicitud.

Si la solicitud es rechazada en presencia del solicitante por inconsistencia de la documentación de respaldo presentada, se le informa en persona al solicitante.

c. **Solicitud en espera.** Si la documentación de respaldo de la solicitud completada tuviera defectos subsanables, todo el trámite queda en espera hasta que el solicitante complete adecuadamente los datos insuficientes o erróneos presentados, quedando en ese caso la documentación correcta en custodia del Oficial de Registro.
El procesamiento de las solicitudes de certificados recibidas que no hayan finalizado dentro de los treinta días de generación quedarán en estado “expirado” de manera automática por el sistema.

4.3 Emisión del certificado.

4.3.1 Proceso de emisión del certificado.

Cumplidos los recaudos del proceso enunciado en el apartado 4.1. solicitud de certificado y una vez aprobada la solicitud de certificado por la Autoridad de Registro correspondiente, la Autoridad Certificante **AC – LAKAUT** emitirá el certificado firmándolo digitalmente y en cumplimiento con la comprobación de la identidad del firmante, confronta mediante reconocimiento facial y datos biométricos de huella dactilar de los solicitantes y suscriptores de certificados de firma digital, utilizando el servicio de verificación de identidad provisto por el REGISTRO NACIONAL DE LAS PERSONAS, poniéndolo a disposición del suscriptor.
En el mismo sentido, se emitirá un certificado ante una solicitud de renovación.

4.3.2 Notificación de emisión.

Una vez finalizado el proceso de solicitud de un certificado, la **AC – LAKAUT**, enviará de manera automática e inmediata al suscriptor del certificado, un correo electrónico notificando de la emisión de su certificado y brindándole el PIN de Revocación. La dirección del correo electrónico al que se notifica la emisión del certificado, fue verificada durante el proceso de solicitud del certificado.

4.4 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.

4.5 Uso del par de claves y del certificado.

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

Según lo establecido en la Ley Nº 25.506, en su artículo 25, el suscriptor debe:
a) Mantener el control exclusivo de sus datos de creación de firma digital, no compartirlos, e impedir su divulgación.

b) Utilizar UN (1) dispositivo de creación de firma digital técnicamente confiable.

c) Solicitar la revocación de su certificado al Certificador ante cualquier circunstancia que pueda haber comprometido la privacidad de sus datos de creación de firma.

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

Asimismo, se indicará que el suscriptor debe cumplir con las siguientes obligaciones:

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

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

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

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

y de cualquier otro documento aplicable.

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

Los Terceros Usuarios deben:

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

b) Verificar la validez del certificado digital.

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

Se aplica el punto 3.3 y 3.4 Generación de UN (1) certificado con el mismo par de claves.

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

En el caso de certificados digitales de Personas humanas, 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 3.4 Autenticación de la identidad de Personas humanas.

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

Para los certificados de aplicaciones, incluyendo los de servidores, los responsables deben tramitar UN (1) nuevo certificado en todos los casos, cumpliendo los pasos requeridos en el apartado 3.3. Autenticación de la identidad de Personas Jurídicas Públicas o Privadas.

4.8 - 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, de existir alguna modificación procede la revocación de dicho certificado y de ser requerido, la solicitud de uno nuevo.

4.9 Suspensión y Revocación de Certificados.

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

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

4.9.1 Causas de revocación.

El Certificador procederá a revocar los certificados digitales que hubiera emitido en los siguientes casos:

a) A solicitud del titular del certificado digital o del responsable autorizado para el caso de los certificados de Personas Jurídicas o aplicación.

b) Si se determina que el certificado fue emitido en base a información falsa, que al momento de la emisión hubiera sido objeto de verificación.

c) Si determina que los procedimientos de emisión y/o verificación han dejado de ser seguros.

d) Por resolución judicial.

e) Por acto administrativo de la Autoridad de Aplicación debidamente fundado.

f) Por fallecimiento del titular.

g) Por declaración judicial de ausencia con presunción de fallecimiento del titular.

h) Por declaración judicial de incapacidad del titular.

i) Si se determina que la información contenida en el certificado ha dejado de ser válida.

j) Cuando la clave privada asociada al certificado, o el medio en que se encuentre almacenada, se encuentren comprometidos o corran peligro de estarlo.

k) Ante incumplimiento por parte del suscriptor de las obligaciones establecidas en el Acuerdo con Suscriptores.

l) Si se determina que el certificado no fue emitido de acuerdo a los lineamientos de la Política Única de Certificación, del Manual de Procedimientos, de la Ley N° 25.506 y su modificatoria, sus normas reglamentarias.

AC - LAKAUT, en caso de corresponder, revocará el certificado en un plazo no superior a las

VEINTICUATRO (24) horas de recibido el requerimiento de revocación.

4.9.2 - Autorizados a solicitar la revocación.

Se encuentran autorizados para solicitar la revocación de UN (1) certificado:

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

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

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

d) El Certificador o la Autoridad de Registro.

e) El Ente Licenciante.

f) La Autoridad Judicial.

g) La Autoridad de Aplicación.

4.9.3 - Procedimientos para la solicitud de revocación.

El certificador garantiza que:

a) Se identifica debidamente al solicitante de la revocación según se establece en el apartado 3.3 y 3.4

b) Las solicitudes de revocación, así como toda acción efectuada por el certificador o la autoridad de registro en el proceso, están documentadas y conservadas en sus archivos.

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

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

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

Las solicitudes de revocación deben poder efectuarse en cualquier Autoridad de Registro, independientemente de en cual se haya emitido el certificado. Los números telefónicos y direcciones de correo electrónico de contacto de cada uno de ellos se encuentran disponibles en el sitio web de la **AC – LAKAUT** (lakautac.com.ar/firma-digital/autoridadesDeRegistro).

Una vez efectuada la revocación, se actualiza el estado del certificado en el repositorio y se

incluye en la próxima lista de certificados revocados a ser emitida.

4.9.4 - Plazo para la solicitud de revocación.

El titular de un certificado debe requerir su revocación en forma inmediata cuando se presente alguna de las circunstancias previstas en el apartado 4.9.1.

El servicio de recepción de solicitudes de revocación se encuentra disponible en forma permanente SIETE POR VEINTICUATRO (7x24) horas cumpliendo con lo establecido en el Artículo 21, Capítulo II inciso 8 del Decreto Nº 182/2019.

4.9.5 - 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.

4.9.6 - Requisitos para la verificación de la lista de certificados revocados.

Los Terceros Usuarios deben validar el estado de los certificados, mediante el control de la lista de certificados revocados, a menos que utilicen otro sistema con características de seguridad y confiabilidad por lo menos equivalentes.
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 21, Capítulo II inciso 9 del Decreto Nº 182/2019 relativo al acceso al repositorio de certificados revocados y las obligaciones establecidas en la presente Resolución 946/2021 y sus correspondientes Anexos.

4.9.7 - 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. Puede verificarse mediante el acceso a la lista de certificados revocados disponible en el sitio https://www.lakautac.com.ar/firma-digital/listadoRevocados

4.9.8 - 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. Se indica la vigencia de cada lista de certificados revocados, y cada lista indica la fecha de emisión de la siguiente.

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

La AC - LAKAUT 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 y de la verificación de estado en línea (OCSP).

El certificador pone a disposición de los terceros usuarios: https://www.lakautac.com.ar/firma-digital/listadoRevocados

a) La información relativa a las características de los servicios de verificación de estado.
b) La disponibilidad de tales servicios y los procedimientos que se seguirán en caso de no disponibilidad.
c) Todas las características opcionales de tales servicios.

Los únicos mecanismos válidos para la verificación del estado de los certificados es a través del servicio OCSP y en su respaldo, las Listas de Certificados Revocados.
En el caso de las aplicaciones propias de **LAKAUT S.A.** donde se utilizan los certificados emitidos por la **AC - LAKAUT,** realizan la consulta sobre la lista de Certificados Revocados en forma automática.

4.9.10 - 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/firma-digital/listadoRevocados

4.9.11 - 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 la presente Política Única de Certificación.

4.9.12 - Requisitos específicos para casos de compromiso de claves.

En caso de compromiso de su clave privada, el titular del certificado correspondiente se encuentra obligado a comunicar inmediatamente dicha
circunstancia al certificador mediante alguno de los mecanismos previstos en el apartado 4.9.2. - Procedimientos para la solicitud de revocación.

4.9.13 - Causas de suspensión.

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

4.9.14 - Autorizados a solicitar la suspensión.

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

4.9.15 - Procedimientos para la solicitud de suspensión.

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

4.9.16 - Límites del periodo de suspensión de un certificado.

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

4.10 - Estado del certificado.

4.10.1 - Características técnicas.

Los servicios disponibles para la verificación del estado de los certificados emitidos por el Certificador son:

- Lista de certificados revocados (CRL). https://www.lakautac.com.ar/firma-digital/listadoRevocados
- Servicio (OCSP). https://www.lakautac.com.ar/crl/lakautac.ocsp/

Respecto a la CRL, se emite cada VEINTICUATRO (24) horas. Con respecto a OCSP, permite verificar si el certificado se encuentra vigente o ha sido revocado en línea. Cada lista CRL indicará la fecha de emisión de la siguiente.

4.10.2 - Disponibilidad del servicio.

Los Servicios descritos en el apartado anterior se encuentran disponibles SIETE POR VEINTICUATRO (7x24) horas, sujetos a un razonable calendario de mantenimiento.

4.10.3 - Aspectos operativos.

No aplica.

4.11 - Desvinculación del suscriptor.

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

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

4.12 - 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.

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

Se describen a continuación los procedimientos referidos a los controles de seguridad física, de gestión y operativos implementados por el certificador. La descripción detallada se efectúa en el Plan de Seguridad.

5.1 - Controles de seguridad física.

Se cuenta con controles de seguridad relativos a:

a) Construcción y ubicación de instalaciones.
b) Niveles de acceso físico.
c) Comunicaciones, energía y ambientación.
d) Exposición al agua.
e) Prevención y protección contra incendios.
f) Medios de almacenamiento.
g) Disposición de material de descarte.
h) Instalaciones de seguridad externas.

5.2 - Controles de Gestión.

- Se cuenta con controles de seguridad relativos a:

a) Definición de roles afectados al proceso de certificación.
b) Número de personas requeridas por función.
c) Identificación y autenticación para cada rol.
d) Separación de funciones.

5.3 - Controles de seguridad del personal

- Se cuenta con controles de seguridad relativos a:

a) Calificaciones, experiencia e idoneidad del personal, tanto de aquellos que cumplen

funciones críticas como de aquellos que cumplen funciones administrativas, de seguridad, limpieza, etcétera.

b) Antecedentes laborales.

c) Entrenamiento y capacitación inicial.

d) Frecuencia de procesos de actualización técnica.

e) Frecuencia de rotación de cargos.

f) Sanciones a aplicar por acciones no autorizadas.

g) Requisitos para contratación de personal.

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

5.4 - Procedimientos de Auditoría de Seguridad.

Se mantienen políticas de registro de eventos, cuyos procedimientos detallados se encuentran en el Manual de Procedimientos.

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

a) Tipo de eventos registrados. Respetando lo establecido en el anexo II, sección 3 de la Resolución 946.

b) Frecuencia de procesamiento de registros.

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

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

e) Procedimientos de resguardo de los registros.

f) Sistemas de recolección y análisis de registros (internos vs. externos).

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

h) Evaluación de vulnerabilidades.

5.5 - Conservación de registros de eventos.

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

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

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

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

a) Tipo de registro archivado. Respetandose lo establecido en el Anexo II Sección 3 de la Resolución 946/2021 de la entonces Secretaría de Innovación Pública de la JEFATURA DE GABINETE DE MINISTROS

b) Periodo de Guarda de los Registros

c) Medidas de Protección de los registros archivados, incluyendo privilegios de acceso

d) Procedimientos de resguardo de los registros.

e) Requerimientos para los registros de certificados de fecha y hora

f) Sistemas de recolección y análisis de registros (internos Y Externos)

g) Procedimientos para obtener y verificar la información archivada

5.6 - Cambio de claves criptográficas.

En todos los casos el **Cambio de Claves Criptográficas de LAKAUT SA** implica la emisión de un nuevo Certificado por parte de la AC Raíz de la República Argentina. Si la Clave Privada de Lakaut SA se encontrase comprometida, se procederá a la revocación inmediata de su Certificado y esa Clave ya no podrá ser usada en el proceso de Emisión de Certificados

El par de claves criptográficas que **LAKAUT S.A.** genera para su Autoridad Certificante (**AC-LAKAUT**) es generado en un ambiente seguro con motivo del licenciamiento de la presente Política Única de Certificación y tendrá una vigencia de CINCO (5) años, al igual que su licencia de Certificador Licenciado.

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

Si por algún motivo resultase necesario cambiar el par de claves de un certificado vigente, el suscriptor deberá solicitar a la **AC - LAKAUT** la revocación de su certificado e iniciar el proceso de solicitud de un nuevo certificado.

5.7- Compromiso y recuperación ante desastres.

Se describen los requerimientos relativos a la recuperación de los recursos del certificador en caso de falla o desastre. Estos requerimientos serán desarrollados en el Plan de Contingencia.

Se han desarrollado procedimientos referidos a:

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

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

c) Recuperación ante compromiso o sospecha de compromiso de la clave privada del certificador.

d) Continuidad de las operaciones en un entorno seguro luego de desastres. Los procedimientos cumplen con lo establecido por el artículo 20 del Decreto Nº 182/2019 en lo relativo a los servicios de infraestructura tecnológica prestados por un tercero.

5.8 - Plan de Cese de Actividades

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

Se han implementado procedimientos referidos a:

a) Notificación al Ente Licenciante, Suscriptores, Terceros Usuarios, otros Certificadores y otros usuarios vinculados.

b) Custodia de archivos y documentación e identificación de su custodio.

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

Se contempla lo establecido por el artículo 44 de la Ley Nº 25.506 de Firma Digital en lo relativo a las causales de caducidad de la licencia. Asimismo, los procedimientos cumplen lo dispuesto por el artículo 20 del Decreto Nº 182/2019, reglamentario de la Ley de Firma Digital, en lo relativo a los servicios de infraestructura tecnológica prestados por un tercero y las obligaciones establecidas en la Resolución 946/2021 de la entonces Secretaría de Innovación Pública de la JEFATURA DE GABINETE DE MINISTROS dependiente de JEFATURA DE GABINETE DE

MINISTRO

6 - CONTROLES DE SEGURIDAD TÉCNICA.

Se describen las medidas de seguridad implementadas por el certificador para proteger las claves criptográficas y otros parámetros de seguridad críticos. Además, se incluyen los controles técnicos que se implementarán sobre las funciones operativas del certificador, Autoridades de Registro, repositorios, suscriptores, etcétera.

6.1 - Generación e instalación del par de claves criptográficas.

La generación e instalación del par de claves deben ser consideradas desde la perspectiva de las autoridades certificantes del certificador, de los repositorios, de las autoridades de registro y de los suscriptores. Para cada una de estas entidades se abordan los siguientes temas:

a) Responsables de la generación de claves.

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

c) Métodos de entrega de la clave pública de la entidad al certificador en forma segura.

d) Métodos de distribución de la clave pública del certificador en forma segura.

e) Características y tamaños de las claves

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

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

6.1.1 - Generación del par de claves criptográficas.

AC - LAKAUT, luego del otorgamiento de la licencia por parte de la Autoridad de Aplicación para esta Política Única de Certificación, es generado el par de claves criptográficas en un ambiente seguro con la participación de personal autorizado, sobre dispositivos criptográficos FIPS 140-2 Nivel 3. Para la generación del par de claves se utilizará el algoritmo RSA de 4096 bits.

En el caso de las Autoridades de Registro, cada Oficial de Registro generará y almacenará su par de claves utilizando un dispositivo criptográfico homologado FIPS 140-2 Nivel 2 o superior y

utilizando el algoritmo RSA con un tamaño mínimo de 2048 bits.

Las claves criptográficas de los suscriptores son generadas y almacenadas por ellos, de acuerdo con los niveles de seguridad establecidos en el apartado 1.3.1. Todos los dispositivos criptográficos, deberán ser homologados por el NIST: National Institute of Standards and Technology, siendo requisito la certificación FIPS 140-2 Nivel 2 para los certificados generados por software o en token criptográfico y de nivel 3 para los generados para ser custodiados por el Certificador Licenciado. Los suscriptores generan sus claves mediante el algoritmo RSA con un tamaño mínimo de 2048 bits.

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 absoluto control. El suscriptor es considerado titular del par de claves; como tal, está obligado a generarlas en un sistema confiable y a no revelar su clave privada a terceros bajo ninguna circunstancia.

Todo ello respetando lo establecido en el Anexo III, Punto 3.2.1 respecto de generación del par de claves (Resolución 946/2021 de la entonces Secretaría de Innovación Pública de la JEFATURA DE GABINETE DE MINISTROS).

6.1.2 - Entrega de la clave privada.

En todos los casos, se cumple con la obligación de lo establecido por la Ley Nº 25.506, artículo 21, inciso b) y el Decreto Nº 182/2019, artículo 21, punto 3).

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

La clave pública del suscriptor del certificado es transferida a la **AC – LAKAUT**, a través de la aplicación correspondiente, durante el proceso de solicitud de su certificado. Para ello, el suscriptor deberá acceder al portal y completados y aprobados por el Oficial de Registro los datos ingresados en la Solicitud de Certificado, que estarán en formato PKCS#[1]10 o bien el formato que lo reemplace en el futuro, una vez comprobada la coincidencia de la clave privada con la pública generada mediante el hash MD5 se realizará la generación del certificado.

6.1.4 - Disponibilidad de la clave pública del certificador.

El certificado del Certificador y su cadena de certificación se encuentran a disposición de los suscriptores y terceros usuarios en un repositorio en línea de acceso público a través de Internet, https://www.lakautac.com.ar/firma-digital/listadoCertificados

6.1.5 - Tamaño de claves.

La longitud de las claves criptográficas del certificado del Certificador es de 4096 bits, con algoritmo RSA.

La longitud de las claves criptográficas de los certificados de suscriptores emitidos por el Certificador es de 2048 bits como mínimo, en algoritmo RSA. y el algoritmo de firma utilizado es SHA-2, respetando lo establecido en el Anexo IV , de la Resolución 946/2021 de la entonces Secretaría de Innovación Pública de la JEFATURA DE GABINETE DE MINISTROS respecto de las longitudes mínimas de las claves.

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 los que corresponden con el algoritmo de generación RSA según su especificación técnica.

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

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

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

La protección de la clave privada es considerada desde la perspectiva del certificador, de los repositorios, de las Autoridades de Registro y de los suscriptores, siempre que sea aplicable. Para cada una de estas entidades se abordan los siguientes temas:

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

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

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

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

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

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

g) Procedimiento de destrucción de la clave privada.

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

6.2.1 – Controles y estándares para dispositivos criptográficos.

Para la generación y el almacenamiento de las claves criptográficas, **AC - LAKAUT**, las Autoridades de Registro y los suscriptores que opten por un nivel de seguridad alto para sus certificados, utilizan los dispositivos criptográficos referidos en el apartado 6.1.1.

Debe respetarse lo establecido en la Resolución 946/2021 de la entonces Secretaría de Innovación Pública de la JEFATURA DE GABINETE DE MINISTROS respecto de los estándares para dispositivos criptográficos.

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. Estos controles son desarrollados con mayor detalle en los documentos específicos, respetando lo definido en el Anexo II de la Resolución 946/2021 de la entonces Secretaría de Innovación Pública de la JEFATURA DE GABINETE DE MINISTROS.

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 - LAKAUT** cuenta con procedimientos para su recuperación. Esta sólo puede ser realizada por personal autorizado, sobre dispositivos criptográficos seguros y exclusivamente en el nivel de seguridad donde se realicen las operaciones críticas de la **AC – LAKAUT.**

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

6.2.4 - Copia de seguridad de clave privada.

Los Procedimientos y Controles de Seguridad empleados para la realización de copias de seguridad de las Claves Privadas del Certificador están diseñadas garantizando que su realización no disminuye los niveles de seguridad de dichas claves por la creación de las citadas copias de seguridad

El Proceso para la generación de la Copia de Seguridad de la **AC – LAKAUT** consiste en la generación de una copia de seguridad de la clave privada del Certificador **LAKAUT S.A.** 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.

6.2.5 - Archivo de clave privada.

Las Claves Privadas de la AC - LAKAUT son archivadas mediante procedimientos ejecutados bajo controles de seguridad que garantizan que no disminuyen los factores de seguridad por el proceso de archivo. Las copias de resguardo de la clave privada de la Autoridad Certificante LAKAUT S.A. son conservadas en lugares seguros, al igual que sus elementos de activación, bajo los niveles de seguridad requeridos por la normativa vigente, descriptos en el Anexo II, de la Resolución 946/2021 de la entonces Secretaría de Innovación Pública de la JEFATURA DE GABINETE DE MINISTROS. El Certificador almacena las copias de resguardo de su clave privada a través de un procedimiento que garantiza su integridad y confidencialidad, conservándola en un lugar seguro, al igual que sus elementos de activación, de acuerdo a lo dispuesto en EL Anexo II de la Resolución citada más arriba de la Secretaría de Innovación Pública en cuanto a los niveles de resguardo de claves..

6.2.6 - Transferencia de claves privadas en dispositivos criptográficos

El par de claves criptográficas del Certificador están generadas y almacenadas en dispositivos criptográficos conforme a lo establecido en la presente Política, no permitiendo su exportación.

6.2.7 - Almacenamiento de claves privadas en dispositivos criptográficos.

Las claves privadas de los suscriptores que tengan dispositivos criptográficos propios son generadas y almacenadas en esos dispositivos y estos estarán homologados como FIPS 140-2 nivel 2 o superior y no permiten su exportación.

6.2.8 - Método de activación de claves privadas.

La clave privada de la **AC – LAKAUT** se activa previa autenticación de los responsables de su

control aplicando un procedimiento seguro que requiere la participación de los poseedores de claves de activación según el control M de N, quienes validan las operaciones críticas, autorizando su ejecución por medio de llaves especiales que obran en su poder.

Los responsables de la activación de las claves privadas deberán identificarse frente al sistema según corresponda al rol asignado y en un orden determinado por medio de distintos mecanismos de autenticación ya sea llaves de seguridad, claves.

Las Autoridades de Registro y los suscriptores de certificados tienen acceso a su clave privada personal a través de una contraseña o PIN de acceso al dispositivo criptográfico y la contraseña de la clave privada.

6.2.9 - Método de desactivación de claves privadas.

La desactivación de la clave privada de la **AC - LAKAUT** se lleva adelante mediante el proceso de desactivación de partición previa autorización de los responsables de su control a través de un procedimiento seguro y cuando se requiera utilizar temporalmente un equipamiento de respaldo o se realicen tareas de mantenimiento.

6.2.10 - Método de destrucción de claves privadas.

En caso de cese de actividades de la **AC – LAKAUT** o de compromiso de su clave privada, se destruirán los dispositivos de soporte de su clave privada mediante un procedimiento que garantice su destrucción total y segura según el último estado del arte disponible a la fecha.

6.2.11 – Requisitos de los dispositivos criptográficos.

Se indican las especificaciones de los dispositivos criptográficos, respetandose lo establecido en el Anexo II, de la Resolución 946/2021 de la entonces Secretaría de Innovación Pública de la JEFATURA DE GABINETE DE MINISTROS respecto de su utilización.

AC - LAKAUT, luego del otorgamiento de la licencia por parte de la Autoridad de Aplicación para esta Política Única de Certificación, ha generado el par de claves criptográficas en un ambiente seguro con la participación de personal autorizado, sobre dispositivos criptográficos FIPS 140-2 Nivel 3. Para la generación del par de claves se utilizará el algoritmo RSA de 4096 bits.

En el caso de las Autoridades de Registro, cada Oficial de Registro generará y almacenará su par de claves utilizando un dispositivo criptográfico homologado FIPS 140-2 Nivel 2 o superior y utilizando el algoritmo RSA con un tamaño mínimo de 2048 bits.

Las claves criptográficas de los suscriptores son generadas y almacenadas por ellos, de acuerdo con los niveles de seguridad establecidos en el apartado 1.3.1. Los dispositivos criptográficos, estos deberán ser homologados FIPS 140-2 Nivel 2 o superior. Los suscriptores generan sus claves mediante el algoritmo RSA con un tamaño mínimo de 2048 bits.

6.3 - Otros aspectos de administración de claves.

6.3.1 - Archivo permanente de la clave pública.

Los certificados emitidos a suscriptores y a los Oficiales de Registro como así también el de la AC LAKAUT son almacenados bajo un esquema de redundancia y respaldados en forma periódica sobre dispositivos de solo lectura, lo cual sumado a la firma de los mismos, garantiza su integridad.

Las políticas y controles de seguridad implementados para recuperar la clave pública archivada, incluyendo el software y hardware, se hallan descriptos en el Plan de Contingencia .

6.3.2 - Período de uso de clave pública y privada.

La clave privada asociada con el certificado digital de la **AC - LAKAUT**, tiene una validez de DIEZ (10) años, y de no mediar una revocación anticipada, se lo utilizará para firmar certificados de suscriptores.

Las claves privadas de los suscriptores, asociadas a los certificados emitidos por la **AC - LAKAUT** se utilizarán únicamente durante su período de validez, que será de DOS (2) años tanto para todos los tipos de certificados. El período de uso de la clave privada y su certificado asociado puede ser extendido por medio de la renovación del certificado de acuerdo con lo establecido en el apartado 4.1.2.

6.4 - Datos de activación.

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

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

6.4.1 - Generación e instalación de datos de activación.

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 la **AC - LAKAUT,** ni las Autoridad de Registro implementan mecanismos de respaldo de contraseñas y credenciales de acceso a las claves privadas de los suscriptores u Oficiales de Registro o a sus dispositivos criptográficos, si fuera aplicable.

6.4.2 - Protección de los datos de activación.

Se indican los procedimientos para garantizar la adecuada protección de los datos de activación contra usos no autorizados.

Las Oficiales de Registro y los Suscriptores son responsables de la custodia de sus respectivos dispositivos criptográficos y de la no divulgación de la contraseña de acceso del dispositivo criptográfico ni de la contraseña de la clave privada.

Ni **LAKAUT S.A.,** ni la Autoridad de Registro Central, ni las Autoridades de Registro Delegadas implementan mecanismos de respaldo de las contraseñas de la clave privada ni de la contraseña de acceso del dispositivo criptográfico de ORs, ni de Suscriptores.

La **AC- LAKAUT** establece los siguientes procedimientos de control sobre su clave privada:

a) se establecen al menos DOS (2) responsables de su control.
b) se establece un procedimiento de activación de clave privada.
c) se establece un procedimiento de destrucción de la clave privada.

Los datos de activación de la clave privada de la **AC - LAKAUT** están protegidos por mecanismos de seguridad implementados en el nivel 6 de máxima seguridad.

6.4.3 - Otros aspectos referidos a los datos de activación.

Es responsabilidad de los Oficiales de Registro y de los suscriptores de certificados emitidos por la **AC - LAKAUT**, elegir contraseñas fuertes para la protección de sus claves privadas y para el acceso a los dispositivos criptográficos que utilicen, si fuera aplicable.

6.5 - Controles de seguridad informática.

6.5.1- Requisitos Técnicos específicos.

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

Dichos requisitos se vinculan con los siguientes aspectos:

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

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

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

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

e) Archivo de datos históricos y de auditoría del certificador y usuarios.

f) Registro de eventos de seguridad.

g) Prueba de seguridad relativa a servicios de certificación.

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

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

Estas funciones son provistas por una combinación del sistema operativo, software de certificación y controles físicos. La descripción de los controles de seguridad establecidos sobre los servidores del Certificador se incluye en el Plan de Seguridad.

6.5.2 - Requisitos de seguridad computacional

El Hardware y el Software que utiliza la Autoridad Certificante Lakaut dispone de las siguientes calificaciones de seguridad, emitidas por las organizaciones descriptas para cada una de ellas:

- HSM Luna SA: Certificado EAL4+
- RedHat Enterprise Linux 6.7: Certificado EAL4+
- RedHat JBOSS Enterprise Application Plataform 6.2: Certificado EAL4+
- PostgreSQL 9.3.2: Sin Certificar
- Switch HP 5120: Sin Certificar

- Firewall CheckPoint OpenServer R 77.20: Certificado EAL+4
- VmWare vSphere 6.0: Certificado EAL+4

6.6 - Controles Técnicos del ciclo de vida de los sistemas

LAKAUT S.A. mantiene el control de los equipos y de la documentación de la configuración de los mismos y de los sistemas instalados que prevén registrar toda modificación o actualización a cualquiera de ellos.

El esquema de seguridad física del SMS (Safety Management System) de la Autoridad Certificante **AC - LAKAUT** previene que terceros no autorizados puedan ingresar indebidamente a sus instalaciones. El control periódico de integridad del sistema de la Autoridad Certificante **AC - LAKAUT** advierte sobre cualquier cambio realizado, lo identifica y permite comprobar su validez.

6.6.1 - Controles de desarrollo de sistemas

El Certificador cumple con procedimientos específicos para el diseño y desarrollo de sistemas entre los que se encuentran:

- Separación de ambientes de desarrollo, prueba y producción
- Control de versiones para los componentes desarrollados

6.6.2 - Controles de gestión de seguridad

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

6.6.3 - Controles de seguridad del ciclo de vida del software

No aplica.

6.7 - Controles de seguridad de red

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

6.8 - Servicio de Emisión de Sello de Tiempo

El servicio de emisión de sellos de tiempo de la **AC - LAKAUT** está basado en la especificación de los estándares RFC 3161 - “Internet X. 509 Public Key Infrastructure Timestamp Protocol“ y a

su especificación equivalente RFC 3628 – “Policy Requirements for time-stamping authorities” y está sincronizado según lo especificado por Anexo II Sección 3 REGISTRO DE EVENTOS - Información Crítica sobre sincronización de eventos de la Resolución 946/2021 de la entonces Secretaría de Innovación Pública de la JEFATURA DE GABINETE DE MINISTROS.
La Hora Universal se tomará desde los servidores Stratum Two NTP Time Servers con base en Buenos Aires, para el sellado de tiempo y la coordinación de la hora en la red de Firma Digital de **AC - LAKAUT** y las Autoridades de Registro delegadas por **AC - LAKAUT**.

Procesamiento de la Solicitud de Certificados de Sello de Tiempo

Para Utilizar el Servicio de Sello de Tiempo de LakautAC, es conveniente poseer un Certificado de Firma Digital Emitido por LakautAC, ya que la aplicación simultánea de ambos garantiza el no repudio .Para acceder, el Usuario debe tener firmado previamente un convenio de Uso del Servicio de Sello de Tiempo(Time Stamping), convenio que lo habilita a acceder a este servicio.

Las solicitudes de sellos de tiempo emitidos bajo esta Política, respetan la sintaxis de la especificación “RFC3161 Time Stamp Protocol (TSP)”.

Los pasos para generar un sello de tiempo son los siguientes:

• El Solicitante con el software propuesto por LakautAC, que manejara en forma automática este proceso, calcula el hash utilizando el algoritmo SHA-1 o SHA2-256 del documento a sellar, según el nivel del Certificado de Firma que dispone.

• El Solicitante envía una solicitud de sello de tiempo a la URL determinada por LakautAC para ese servicio, siguiendo el protocolo RFC 3161, incluyendo el hash del documento a sellar.

• El Software de Sello de Tiempo de LakautAC recibe la petición, revisa si la petición está completa y correcta.

- Si el resultado es correcto, LakautAC firma la petición generando un Sello de Tiempo (incluyendo el hash del documento, la fecha y hora obtenida de su Servidor de Sello de Tiempo, y lo firma Digitalmente con su Certificado de Certificador Licenciado.

- El sello de tiempo se envía de vuelta al solicitante.

- El Solicitante, informado por su software para solicitar sellos de tiempo de la recepción de la respuesta, debe, si el software le informa que su solicitud fue aprobada por LakautAC, validar la firma del sello y aplicarlo con su firmador en el documento que dio origen a la solicitud de certificación de tiempo.

La URL del servicio de Sellado de Tiempo se encontrará publicada en el sitio Web de LakautAC y debidamente expresada en el correspondiente Convenio de Servicio de Sellado de Tiempo, al que se accede con un PIN de su exclusivo conocimiento.

Respuesta del Certificador Licenciado LakautAC a la solicitud de Sellos de tiempo:

- Si la solicitud no se puede procesar, se devuelve al programa informático de solicitud de sello de tiempo del solicitante una respuesta http indicando con una breve descripción del error la causa. Esta respuesta será enviada, cada vez que LakautAC no pueda responder con un time stamp.

Los posibles errores son:

Causa	Descripción
Cliente envía petición GET	METHOD NOT VALID
Falta el campo content-length	CONTENT_LENGTH REQUIRED
Content-length demasiado grande	REQUEST ENTITY TOO LARGE
Content-type incorrecto	UNSUPORTED MEDIA TYPE
Los datos no son un time stamp request	BAD REQUEST
El servidor no responde	SERVER INTERNAL ERROR

Las respuestas se envían en el siguiente formato:

Content type: ***application/timestamp-reply*** ***Method:*** ***POST*** ***Content-length: required***
<< Contiene la respuesta de sello de tiempo en ASN.1, codificado en DER>>

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

Los Certificados de Competencia o, Sello de Competencia, tienen una estructura similar a los Certificados de Firma Digital, sólo que no contienen clave pública. Un Sello de Competencia contiene atributos que especifican la pertenencia a un grupo, un rol u otra información de autorización relacionada con su titular.

Los Certificados de Sellos de Competencia x509 permiten proveer varios servicios de identificación asociados unívocamente a su portador, desde capacidades profesionales formales registradas, hasta permisos de seguridad para el Uso o Acceso a la información por cuestiones legales previstas en la Ley de Protección de Datos Personales ,la de Protección de Datos del

Paciente en Medicina o incluso seguridad incluyendo control de acceso, con autenticación del origen de los permisos y no repudio.

El estar este tipo de Certificado X509 definido en la Resolución 946/2021 de la entonces Secretaría de Innovación Pública de la JEFATURA DE GABINETE DE MINISTROS, como parte de la Infraestructura de Firma Digital de la República Argentina permite relacionarlo con el Certificado de Firma Digital del titular ,lo que admite que, al usarlos, se pueda, además validar que la persona que aplica la firma está autorizada a firmar invocando ese rol, que sea quien dice ser y no puede negar el acto de firma.

Prestador de servicios de terceros de confianza.
Para la emisión, guarda y verificación de Sellos de Competencia a autoridades de competencia habilitadas.

RESUMEN DEL CERTIFICADO DE SELLO de COMPETENCIA emitidos por Autoridades de Competencia con Convenio con AC-LAKAUT.

El Certificador Licenciado LakautAC Presta Servicios de Confianza a las Autoridades de Sellos de Competencia, con la incumbencia definida para ese Servicio por la Resolución 946/2021 de la entonces Secretaría de Innovación Pública de la JEFATURA DE GABINETE DE MINISTROS de la JGM para los Certificadores Licenciados Privados. El Convenio a celebrar debe ser Aprobado previo a su puesta en marcha, por la Secretaría de Innovación Pública de la JGM mediante Resolución, En el mismo se Regulan los requisitos a ser observados por los Emisores de Sellos de Competencia autorizados por la Secretaría de Innovación Pública de la JGM de en los procesos de Emisión, Guarda y Verificación de Certificados de Sellos de Competencia en el ámbito de LakautAC,o en Instalaciones de la Autoridad de Competencia, respecto a:

a) algoritmos y parámetros para la creación de certificados de Sellos de Competencia;
b) formato y forma de crear un certificado de Sello de Competencia;
c) procedimiento de verificación y condiciones para la validación de un certificado de Sello de Competencia.

Según lo definido en la Resolución 946/2021 de la entonces Secretaría de Innovación Pública de la JEFATURA DE GABINETE DE MINISTROS, el formato, los Procedimientos y la estructura que se utilizará para la creación del certificado de Sello de Competencia se siguen las

especificaciones contenidas en la citada Resolución y en la RFC 5755.

Las pautas contenidas en este Acápite son observadas por todas las entidades que celebren acuerdos de Servicios de Confianza para la Emisión y/o Guarda y Administración de Sellos de Competencia con LakautAC, en particular por los desarrolladores de aplicaciones para la emisión, almacenamiento y verificación del certificado de Sello de Competencia emitido por una Entidad Emisora de Sellos de Competencia habilitada por la Secretaría de Innovación Pública, según lo establecido en la Resolución 946/2021 de la entonces Secretaría de Innovación Pública de la JEFATURA DE GABINETE DE MINISTROS y la RFC-5755.

Las Definiciones que continúan en los Acápites 2 y 3 corresponden a: El Acápite 2 presenta el perfil del Certificado de Sello de Competencia considerando la estructura lógica y la estructura de implementación; y el Acápite 3 lista las recomendaciones para la emisión, almacenamiento y verificación del Certificado de Sello de Competencia.

Certificados de sello de competencia - DEFINICIÓN

Todo Certificado de Sello de Competencia es emitido por una institución, caracterizada dentro del alcance de la Resolución 946/2021, a partir de su habilitación.

Cualquier información bajo la gestión de una Entidad Habilitada para Emitir Sellos de Competencia, relativa a un ciudadano o una empresa, puede incluirse en un certificado de Sellos de Competencia, siempre que la Entidad Habilitada sea el administrador y legalmente responsable de la información contenida, en el Sello de Competencia su Emisión y Almacenamiento.

Un Sello de Competencia-SC es un documento electrónico en formato X.509 firmado por un certificado digital emitido por un Certificador Licenciado habilitado por la Secretaría de Innovación Pública de la JGM. Este documento electrónico contendrá información sobre una situación o calificación específica de un ciudadano o una empresa.

El contenido de un Certificado de Autoridad de Sello de Competencia, siempre está firmado por un Certificado Digital de Jurídica emitido por un Certificado Licenciado de Firma Digital Autorizado por la Autoridad Certificante, lo que le otorga garantías técnicas y legales en cuanto a su uso y aplicación por la sociedad en general.

Quienes posean y deban asociar un certificado de firma digital a un Sello de Competencia, deben solicitar un nuevo certificado de firma, ya que este debe tener marcado el bit digitalSignature en la extensión "uso de clave" (keyUsage) y, además, debe asegurarse de que el Certificador le asigne un número de Serie al de Firma distinto al del Sello de Competencia, para evitar inconvenientes con las consultas de validez y las revocaciones.

Tipos de certificados

Según lo establecido en la Resolución 946/2021 de la entonces Secretaría de Innovación Pública de la JEFATURA DE GABINETE DE MINISTROS, el certificado de Sello de Competencia emitido siguiendo las recomendaciones y estándares de la RFC 5755.

Estructura lógica del certificado de Sello de Competencia

Los certificados de sellos de competencia se utilizan en una amplia gama de aplicaciones y entornos que cubren un amplio espectro de objetivos de interoperabilidad y requisitos operativos y de seguridad. El propósito de este acápite es establecer una línea de base común para aplicaciones genéricas que requieren una amplia interoperabilidad.

Los principales campos de datos / información contenidos en un Certificado de Sello de Competencia se describen a continuación con el fin de proporcionar una guía adecuada para la emisión de un SC por parte de un Emisor Autorizado por la Secretaría de Innovación Pública a esos fines, dentro del alcance de lo reglamentado en la Resolución 946/2021 y la RFC 5755.

EMISOR: es toda entidad que gestiona determinada información que puede ser tratada en formato SC(Sello de Competencia) de acuerdo con lo normado en la Resolución 946/2021 de la entonces Secretaría de Innovación Pública de la JEFATURA DE GABINETE DE MINISTROS, es decir, la Autoridad de Competencia. Debe utilizar el nombre asignado en la Resolución Habilitante como Autoridad de Competencia y la Resolución Habilitante asociada para una identificación inequívoca.

TITULAR DEL CERTIFICADO DE COMPETENCIA: es la persona o institución que posee el certificado de competencia. El nombre debe usarse precedido de una identificación única que permita la caracterización completa del titular. Algunas competencias públicas se admiten como identificación única, entre ellos: CPN, Médico, Abogado; o la identificación única utilizada por los

Organismos de Emisión y Control de Matrículas Profesionales para gestionar la información sobre el titular del Sello de Competencia, incluidos: Número de Registro o Número de Matrícula u otra información de calificación e identificación con los Registros Profesionales sobre el titular del Certificado de Sello de Competencia.

PERÍODO DE VIGENCIA: todo certificado debe tener necesariamente una vigencia entre un período de tiempo. Se deben considerar la fecha y hora de inicio y la fecha y hora de finalización de la validez del Certificado de Sello de Competencia.

NÚMERO DE SERIE: cada Sello de Competencia emitido por cada Organismo Habilitado debe tener un número de serie único correspondiente a su emisión para permitir el control y gestión de los certificados emitidos por cada Autoridad de Competencia habilitada por la Secretaría de Innovación Pública, además de facilitar el proceso de VALIDACIÓN sin necesidad de especificar otra información contenida en un SC.

TIPO DE CERTIFICADO DE SELLO de COMPETENCIA: la Autoridad de Competencia debe especificar el tipo de SC que se emite, ya sea SCA o SCV.
COMPETENCIA/S: en este campo la Autoridad de Competencia establece la finalidad principal del Certificado de Sello de Competencia. Este contenido explica la calificación del TITULAR DEL CERTIFICADO DE SELLO DE COMPETENCIA. La información contenida en este campo permitirá el uso y tratamiento adecuado del SC por parte de la Autoridad de Competencia y también cuando se presente a un tercero para la calificación del titular del SC. Los atributos admisibles para este campo son: Información del servicio de autenticación, ID de acceso, ID de tarea, Grupo, Rol y Nivel de acceso.

FIRMA DIGITAL DE AUTORIDAD DE COMPETENCIA: se trata de información fundamental que debe estar Emitida y Certificada por un Organismo Habilitado y Reconocido por la Legislación Vigente para así Garantizar la autenticidad y validez legal del Certificado de Sello de Competencia emitido.
EXTENSIÓN: Este campo describe la información necesaria mediante la cual el SC debe ser verificado, y necesaria en caso de que la Autoridad de Sello de Competencia establezca condiciones de revocación del SC antes de que expire la vigencia. Cada solicitud debe considerar este campo, junto con las otras formas de verificación del SC para la autenticidad, integridad y validez técnica y legal. Este campo debe contener la clave de acceso a la Lista de Certificados

de Sellos de Competencia Revocados cuando lo defina la Autoridad Certificante de Competencia.

VERSIÓN: este campo debe ser llenado con la versión V2, según RFC 5755.

PERFIL DE CERTIFICADO DE SELLO DE COMPETENCIA

Este Párrafo presenta el perfil del Certificado de Competencia que promueven su interoperabilidad y la adecuada aplicación en el ámbito de los Certificados Emitidos por las Autoridades de Competencia Habilitadas por la Secretaría de Innovación Pública de la JGM para ser utilizados por la sociedad en general. Este documento también define algunas extensiones privadas para la comunidad de Internet.

Estos Sellos se basan en las Normas ISO / IEC / ITU en su versión 1993 (o posterior) de ASN.1, en este acápite se utiliza dicha sintaxis ASN.1 , como se hace para los Certificados de clave pública [PKIXPROF].
Cuando se especifican longitudes de campo máximas, se refieren a tamaños para la codificación DER y no incluyen la etiqueta o la longitud de campo de la sintaxis ASN.1.

Los certificados de Sellos de Competencia deben ajustarse al formato definido por el estándar ITU X.509 o ISO / IEC 9594-8, que contiene los siguientes campos:

AttributeCertificate :: = SEQUENCE {
acinfo AttributeCertificateInfo,
signatureAlgorithm AlgorithmIdentifier,
signatureValue BIT STRING}
AttributeCertificateInfo :: = SEQUENCE {
versión AttCertVersion, - la versión es v2
titular titular,
emisor AttCertIssuer,
Firma AlgorithmIdentifier,
serialNumber CertificateSerialNumber,
attrCertValidityPeriod AttCertValidityPeriod,
Competencia SECUENCIA DE Competencia,
extensiones Extensiones OPCIONAL}

AttCertVersion :: = INTEGER {v2 (1)}
Titular :: = SECUENCIA {
baseCertificateID [0] IssuerSerial OPCIONAL,
- el emisor y el número de serie de
- Certificado de clave pública del titular
entityName [1] GeneralNames OPCIONAL,
- el nombre del demandante o función
objectDigestInfo [2] ObjectDigestInfo OPCIONAL
- utilizado para autenticar directamente al titular,
- por ejemplo, un ejecutable}
ObjectDigestInfo :: = SECUENCIA {
digestedObjectType ENUMERATE {
publicKey (0),
publicKeyCert (1),
otherObjectTypes (2)},
- otherObjectTypes NO DEBE- ser utilizado en este perfil
otherObjectTypeID IDENTIFICADOR DE OBJETO OPCIONAL,
digestAlgorithm AlgorithmIdentifier,
objectDigest BIT STRING}
AttCertIssuer :: = CHOICE {
v2Form [0] V2Form: solo v2}
V2Form :: = SECUENCIA {
issuerName GeneralNames OPCIONAL,
baseCertificateID [0] IssuerSerial OPCIONAL,
objectDigestInfo [1] ObjectDigestInfo OPCIONAL
- issuerName DEBE estar presente en este perfil
- baseCertificateID y objectDigestInfo NO DEBEN
- estar presente en este perfil}
IssuerSerial :: = SECUENCIA {
emisor GeneralNames,
serial CertificateSerialNumber,
issuerUID UniqueIdentifier OPCIONAL}
AttCertValidityPeriod :: = SECUENCIA {
notBeforeTime GeneralizedTime,

notAfterTime GeneralizedTime}
Atributo :: = SECUENCIA {
tipo AttributeType,
valores SET OF Competence-AttributeValue
- se requiere al menos un valor}
Competence-AttributeType :: = IDENTIFICADOR DE OBJETO
Competence-AttributeValue :: = CUALQUIER DEFINIDO POR Competence-AttributeType

Dentro del alcance de este párrafo, al menos los siguientes campos deben estar contenidos en un certificado de Sello de Competencia, estándar aprobado por la Secretaría de Innovación Pública:

1	Versión	Versión
2	Titular del certificado de competencia	poseedor
3	Editor	Editor
4	algoritmo de firma	Firma
5	Número de serie	número de serie
6	Período de validez	attCertValidityPeriod
7	Competencias	Competencias
8	Extensiones	Extensiones
9	Firma digital	SignatureValue

Competencia - Certificado Titular

El campo del titular contiene la información de identificación del titular. Se puede representar de tres formas: baseCertificateID, entityName u objectDigestInfo, es decir, según la identificación de un certificado, según el nombre de una entidad o según la información resumida de un objeto, respectivamente.
Se recomienda que solo se utilice uno de los formularios para evitar ambigüedades.

Para SCV, el formulario vinculado al certificado digital se define mediante el campo baseCertificateID. El campo emisor del certificado digital - SC no estará vacío y será único. Los campos del número de serie y del emisor del SC deben coincidir con el campo del titular de la Autoridad de Competencia.

Para CAV, el formulario basado en un nombre de entidad se define mediante el campo entityName . El campo entityName será el mismo que el campo subject en el Certificado Digital del titular de la Competencia atributo o uno de los valores de la extensión subjectAltName (si la extensión existe).

También, es posible que CAV forme un formulario basado en información de resumen de un objeto que se define mediante el campo objectDigestInfo. Este formulario se utiliza en los casos en que el Sello de Competencia no está vinculado ni por el nombre de identificación (a través de entityName) ni por la identificación mediante un Certificado Digital de Firma (a través de baseCertificateID). En este caso, se realiza un enlace entre el objeto y el certificado de Sello de Competencia, agregando el resumen criptográfico (hash) del objeto en el campo titular de la Autoridad Certificante de Competencia.

Para vincular el Sello de Competencia a un Certificado de Firma Digital a través de un resumen criptográfico

Esto se calculará en la codificación DER de todo el Certificado de Firma Digital, incluido el signatureValue . En este caso, el digestedObjectType debe ser " publicKeyCert ". Para digerir criptográficamente la unión de única clave pública del titular del Certificado de Firma Digital , el digestedObjectType debe ser " clave pública " y el resumen debe calcularse sobre la clave pública del titular sólo de su Certificado de Firma Digital. En cualquier caso, para cumplir con este documento, el campo otherObjectTypeID no estará presente.

Emisor

El campo del emisor debe contener el nombre único (nombre distinguido-DN) del emisor y no debe estar vacío. Las Certificadoras de Sellos de Competencia omiten los campos baseCertificateID y objectDigestInfo .

Algoritmo de firma - firma

Contiene el identificador del algoritmo utilizado para validar la firma de la Autoridad de Competencia. Este algoritmo es uno de los algoritmos definidos en la Resolución 946/2021 y el RFC 5755.

Número de serie - serialNumber

Todas las Autoridades de Competencia deben tener un par ÚNICO emisor / número de serie , incluso si el Sello de Competencia es de corta duración. El serialNumber debe ser un número entero positivo con un límite máximo de hasta 20 octetos.

Período de vigencia: attCertValidityPeriod

Este campo define el período durante el cual el emisor del Sello de Competencia certifica que los vínculos entre el titular y el campo de competencia serán válidos. Este período viene dado por el intervalo notBefore y NotAfter . Debe tener el formato GeneralizedTime , estándar ASN.1 y expresado en UTC (Universal Time Coordinated) AAAAMMDDHHMMSSZ.

Competencia-Atributos

El campo proporciona las competencias-atributos,segun información proporcionada al titular de la Autoridad de Competencia. Si se usa para autorización, contiene un conjunto de privilegios.

Un Sello de Competencia contendrá al menos una competencia. Cada competencia contiene el tipo de competencia y un conjunto de valores.

Tipos de Competencias

Algunos de los tipos de Competencias definidos a continuación utilizan el tipo IetfAttrSyntax , también definido a continuación. Las razones para utilizar este tipo son:

1. Permite una separación entre el emisor de competencias y la Autoridad de Política de Competencias. Esto es útil para situaciones en las que una sola autoridad política (por ejemplo, una organización) asigna valores de competencia, pero en las que se despliegan múltiples Autoridades de Competencia para un mejor rendimiento o por otras razones.

2. Las sintaxis permitidas para los valores están restringidas a OCTET STRING, OBJECT IDENTIFIER , UTF8String, que reducen significativamente la complejidad asociada con las correspondientes sintaxis más generales. Todas las competencias de varios valores que utilizan una sintaxis estricta para cada valor utilizan la misma opción de sintaxis de valor. Por ejemplo, los emisores de Sellos de Competencia no deben usar un valor con un OID y un segundo valor con una cadena.

IetfAttrSyntax :: = SECUENCIA {

policyAuthority [0] GeneralNames OPCIONAL,
valores SECUENCIA DE ELECCIÓN {
octetos OCTET STRING,
oid IDENTIFICADOR DE OBJETO,
cadena UTF8String
En las descripciones siguientes, cada tipo de competencia está marcado como "Múltiples permitidos" o "Sólo un valor de competencia; múltiples valores dentro de IetfAttrSyntax". Esto se refiere al conjunto de AttributeValues ; la AttributeType todavía se produce sólo una vez, como se especifica en RFC 5755 .

Información del servicio de autenticación

El atributo SvceAuthInfo identifica al titular de la Autoridad de Competencia para el servidor / servicio por un nombre, y el atributo CAN incluye información de autenticación específica del servicio opcional. Por lo general, contendrá un par de nombre de usuario / contraseña para una aplicación "heredada".

Este atributo proporciona información que puede ser presentada a un verificador de Autoridad de Competencias para ser interpretada y autenticada por una aplicación separada dentro del sistema de destino. Tenga en cuenta que este es un uso diferente al del atributo accessIdentity que se describe a continuación.

Este tipo de atributo normalmente se cifrará cuando el campo authInfo contenga información confidencial, como una contraseña.

nombre id-aca-authenticationInfo
OID {ac-id 1}
sintaxis SvceAuthInfo
Se permiten varios valores
SvceAuthInfo :: = SECUENCIA {
Nombre general del servicio,
ident GeneralName,
authInfo OCTET STRING OPCIONAL}

Identificación de acceso

El atributo accessIdentity identifica al titular del Sello de Competencia para el servidor / servicio. Para este atributo, el campo authInfo no está presente.

Este atributo se utiliza para proporcionar información sobre el titular del Sello de Competencia, que puede ser utilizada por el verificador de la Autoridad de Competencia (o un sistema más

grande del cual el verificador de la Autoridad de Competencia es un componente) para autorizar las acciones del titular del Sello de Competencia dentro de un sistema de verificación de la Autoridad de Competencia. Tenga en cuenta que este es un uso diferente al del atributo svceAuthInfo descrito anteriormente.

nombre id-aca-accessIdentity

OID {ac-id 2}

sintaxis SvceAuthInfo

valoresMúltiples permitidos

Identificación de titularidad

El atributo chargeIdentity identifica al titular del Sello de Competencia a efectos de delegación. En general, la identidad del titular será diferente de las demás identidades del titular. Por ejemplo, la empresa del titular puede estar a cargo del servicio.

nombre id-aca-chargeIdentity

OID {ac-id 3}

sintaxis IetfAttrSyntax

valoressolo un valor de competencia; varios valores dentro de IetfAttrSyntax

Grupo

La competencia de grupo brinda información sobre la pertenencia al grupo del titular del Sello de Competencia.

nombre ID de grupo

OID {ac-id 4}

sintaxis IetfAttrSyntax

los valores son únicamente un valor de competencia; varios valores dentro de IetfAttrSyntax

Ocupación

El atributo de función , especificado en X.509-2000 , aporta información sobre la función asignada al titular del Sello de Competencia.

La sintaxis utilizada para este atributo es:

RoleSyntax :: = SECUENCIA { roleAuthority [0] GeneralNames OPCIONAL, roleName [1] GeneralName}

El campo roleAuthority se especifica la autoridad que emitió el certificado de tipo de rol.

Nivel de acceso

La Competencia-El atributo de autorización , especificado en [X.501-1993], proporciona información de nivel de acceso (asociada con la clasificación de seguridad) del titular del Sello de Competencia.

El campo policyId se utiliza para identificar la política de seguridad a la que se refiere el nivel de acceso. El policyId indica la semántica de los ClassList y securityCategories campos .

Esta especificación incluye el campo classList exactamente como se especifica en X.501-1993 [5]. Los valores adicionales en la clasificación de seguridad y su posición en la jerarquía de clasificación se pueden definir mediante una política de seguridad como asunto local o por acuerdo bilateral. La jerarquía básica de clasificación de seguridad es, en orden ascendente: sin marcar, sin clasificar, restringido, confidencial, secreto y alto secreto.

Una organización puede desarrollar su propia política de seguridad que defina los valores de clasificación de seguridad y sus significados. Sin embargo, la posición BIT STRING de 0 a 5 está reservada para la jerarquía de clasificación de seguridad básica.

Si está presente, el campo SecurityCategory proporciona información de autorización adicional. La política de seguridad identificada por el campo policyId indica las sintaxis que pueden estar presentes en SET securityCategories . Un IDENTIFICADOR DE OBJETO identifica cada una de las sintaxis permitidas. Cuando una de estas sintaxis está presente en SET securityCategories , el OBJECT IDENTIFIER asociado con la sintaxis se carga en el campo SecurityCategory.type .

El identificador de objeto para la Competencia- atributo de autorización de X.509-1997 [6] es:

id-at-clearance IDENTIFICADOR DE OBJETO :: = {

joint-iso-ccitt (2) ds (5) atributoTipo (4) autorización (55)}

La sintaxis asociada es la siguiente:

Liquidación :: = SECUENCIA {

policyId IDENTIFICADOR DE OBJETO,

classList ClassList DEFAULT {sin clasificar},

securityCategories CONJUNTO DE SecurityCategory OPCIONAL}

Las implementaciones soportan el atributo Permiso (autorización) definido en X.501-197 [5]. Las implementaciones no codifican el atributo Liquidación como se define en RFC3281 [7].

ClassList :: = BIT STRING {

sin marcar (0),

sin clasificar (1),

restringido (2),

confidencial (3),

secreto (4),

alto secreto (5)}
SecurityCategory :: = SEQUENCE {
escriba [0] IDENTIFICADOR DE OBJETO,
valor [1] EXPLÍCITO DEFINIDO POR CUALQUIER tipo}

Acceso a la información de la autoridad

El authorityInfoAccess extensión , como se define en [PKIXPROF], se puede utilizar para ayudar al Verificador de Sellos de Competencia sobre el estado de revocación del sello de Competencia. La compatibilidad con id-ad-caIssuers accessMethod es OPCIONAL para este perfil ya que no se esperan cadenas de Sellos de Competencia.

El siguiente método de acceso se utiliza para indicar que la verificación del estado de revocación se proporciona para este Sello de Competencia mediante el Protocolo de estado de certificado en línea (OCSP) definido en [OCSPA]:

id-ad-ocsp IDENTIFICADOR DE OBJETO :: = {id-ad 1}

La ubicación de acceso contiene un URI, y el URI contiene una URL HTTP [URL HTTP] que especifique la ubicación de un respondedor OCSP. El emisor del Certificado de Competencia mantiene un respondedor OCSP en esta ubicación.

nombre id-ce-AuthorityInfoAccess
OID {pe-id 1}
sintaxis AuthorityInfoAccessSyntax
la criticidad es falsa

Puntos de distribución LCR

La extensión cRLDistributionPoints , como se define en [PKIXPROF], Se utiliza para ayudar al verificador de Sellos de Competencia del estado de revocación del Sello de Competencia.

Si la extensión cRLDistributionPoints está presente, entonces está presente exactamente un punto de distribución. La extensión cRLDistributionPoints usa la opción DistributionPointName , que contiene un nombre completo, que contiene un formato de nombre único. Este nombre contiene un DN o un URI. El URI es una URL HTTP [URL HTTP] o una URL LDAP (Protocolo ligero de acceso a directorios) [LDAP-URL].

Nombre ID-ce-cRLDistributionPoints
OID {ce-id 31}
sintaxis cRLDistributionPoints
criticidad es falso

Revocación no disponible

La extensión noRevAvail , definida en X.509-2000, permite a un emisor de Sellos de Competencia indicar que no se pondrá a disposición de este Sello de Competencia información de revocación.

Esta extensión es no crítica. Un verificador de Sellos de Competencia que no comprenda esta extensión puede encontrar una lista de revocación del emisor de Sellos de Competencia, pero la lista de revocación nunca incluirá una entrada para el Sello de Competencia.

nombre id-ce-noRevAvail

OID {ce-id 56}

sintaxis NULL (es decir, '0500'H es codificación DER)

criticidadDEBE ser falso

8.13.5.9 Firma digital del EEE

a) el período de validez de la Competencia- atributo;

b) el período de validez de los Sellos de Competencia que contienen la competencia: el período de validez de los Sellos de Competencia puede ser igual o menor que el período de validez de l a Competencia, siempre que se verifique el estado de revocación. Es posible que la validez del Sello de Competencia sea cuestión de minutos u horas y no requiera el control del estado de revocación;

c) soporte o no soporte de la revocación de competencias: cuando se admite la revocación, condiciones de revocación y reglas de revocación;

d) la posibilidad de obtener una competencia junto con otras a través de un subconjunto de competencias. Cuando esto ocurre, es necesario especificar cómo se puede obtener este subconjunto;

e) la posibilidad de delegar una Competencia: el nombre de la persona que delega es rastreable y los métodos para rastrearlo se indican. Se indicará si existen restricciones, como la aplicabilidad de las políticas de firma, en la aplicación de la delegación. A - Aasignature Contiene la firma digital de la Autoridad de Competencia.

REQUISITOS PARA LA GENERACIÓN Y VALIDACIÓN DE CERTIFICADOS DE SELLOS DE COMPETENCIA

Los procesos relacionados con el ciclo de vida de un certificado de Sello de Competencia pueden identificar y manipular certificados de Competencia emitidos por Autoridades de Competencia Habilitadas por la Secretaría de Innovación Pública de la JGM, así como sus extensiones,

campos y "campos específicos habilitados por la Resolución 946/2021 de la entonces Secretaría de Innovación Pública de la JEFATURA DE GABINETE DE MINISTROS.

En los procesos relacionados con el ciclo de vida del certificado de competencia, por medios técnicos y procedimentales, se cumplen los siguientes requisitos:
a) la firma digital está protegida contra falsificaciones;
b) el contenido digital firmado está protegido contra alteraciones;
c) cualquier componente de software o hardware utilizado no altera el contenido digital;
d) cualquier componente de software o hardware utilizado no impide que el contenido digital se presente y visualice antes y después de cada uno de los procesos relacionados con el ciclo de vida de la firma digital.

Requisitos de la entidad emisora de certificados de Sellos de Competencia:

La Autoridad Emisora de Sellos de Competencia indica en cada Sello de Competencia emitido cuál de las alternativas sigue:
a) verificación de competencias solo en el registro inicial, sin soporte de revocación;
b) verificación de competencias solo en el registro inicial, con soporte para revocación;
c) verificaciones de competencia posteriores, con soporte de revocación y, cuando corresponda, un período de tiempo para la verificación.

Para cualquier competencia, cuando lo admita la Autoridad de Competencia, especifíca en su política, cuando corresponda:
a) el período de validez del atributo;
b) el período de validez de los Sellos de Competencia que contienen la competencia: el período de validez del Sello de Competencia puede ser igual o menor que el período de validez de la Competencia, siempre que se verifique el estado de revocación. Es posible que la validez del Sello de Competencia sea cuestión de minutos u horas y no requiera el control del estado de revocación;
c) soporte o no soporte de la revocación de competencias: cuando se admite la revocación, condiciones de revocación y reglas de revocación;
d) la posibilidad de obtener una Competencia junto con otras a través de un subconjunto de Competencias. Cuando esto ocurre, es necesario especificar cómo se puede obtener este subconjunto.
e) la posibilidad de delegar una Competencia: el nombre de la persona que delega es rastreable

y los métodos para rastrearlo se indican. Se indica si existe alguna restricción, como la aplicabilidad de las políticas de suscripción, al aplicar la delegación.

Perfil del certificado digital de la Autoridad de Competencia

El Certificado digital aplicado al Certificado de Competencia al emitirlo la Autoridad de Competencia cumple con [PKIXPROF] y la extensión keyUsage del Certificado Digital de la Autoridad de Competencia no idica explícitamente que la clave pública de la Autoridad de Competencia no se puede utilizar para validar una firma digital. Para evitar confusiones con respecto a los números de serie y las revocaciones, una Autoridad de Competencia no es también un Certificador Licenciado emisor de certificados de Firma Digital. Es decir, un emisor de Certificados de Sellos de Competencia, tampoco puede ser una autoridad de certificación, emisora de Certificados de Firma Digital es decir, una CA. Por lo tanto, el certificado digital - CD del emisor del certificado de Competencia - CA no tiene una extensión BasicConstraints con el conjunto booleano EEA cA que indica falso.

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

Los certificados emitidos por el Certificador respaldados por esta Política Única de Certificación cumplen con los requerimientos de la Resolución 946/2021 de la entonces Secretaría de Innovación Pública de la JEFATURA DE GABINETE DE MINISTROS y lo establecido en la especificación ITU X509 versión 3 (ISO/IEC 9594-8), adoptada como Estándar Técnico de la Infraestructura de Firma Digital de la República Argentina.

El Certificador adhiere a las recomendaciones de los siguientes documentos en relación al perfil de los certificados:

- RFC 3739 “Internet X.509 Public Key Infrastructure Qualified Certificates Profile” [RFC3739].
- RFC 5280 “Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile” [RFC5280].
- RFC 6960 “X.509 v3 Internet Public Key Infrastructure online Certificate Status Protocol-OCSP”

7.1 - Perfil del certificado.

Todos los certificados son emitidos conforme con lo establecido en la especificación ITU X.509 versión 3 o la que, en su defecto, determine la Secretaría de Innovación Pública, y cumplen con las indicaciones establecidas Sección 2 - “Perfil de certificados digitales” del Anexo IV - Perfiles de los Certificados y de las Listas de Certificados Revocados de la Resolución SIP N° 946/2021 de la entonces Secretaría de Innovación Pública de la JEFATURA DE GABINETE DE MINISTROS.

A) Los siguientes campos se encuentran presentes en los certificados emitidos a **personas humanas** por la **AC – LAKAUT**:

Certificado X.509 v3 Atributos / Extensiones	**Contenido**
Versión (Versión)	Valor 2 que corresponde a Versión 3
Número de serie (SerialNumber)	Entero positivo asignado unívocamente por la AC-LAKAUT a cada certificado
Algoritmo de Firma (SignatureAlgorithm)	Algoritmo usado por el certificador para firmar. Puede ser SHA-1.
Nombre distintivo del emisor (Issuer DN)	CN = AC-LAKAUT SERIALNUMBER = CUIT 30710964277 O = LAKAUT S.A. S = Ciudad Autónoma de Buenos Aires C = AR
Validez (desde, hasta) (Valid From / Valid To)	2 años

Nombre distintivo del suscriptor (Subject DN)	CN = Nombre que figura en el Documento de Identidad del suscriptor. SERIALNUMBER = Tipo y número de identificación del titular 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. • "EX" [país]: Número y tipo de documento extranjero aceptado en virtud de acuerdos internacionales. C = AR
Clave pública del suscriptor (Subject Public Key Info)	Tipo de algoritmo: RSA Longitud de clave: 2048 Bits
Extensiones	
Identificador de la clave de la Autoridad Certificante (Authority Key Identifier)	Contiene un hash de 20 bytes del atributo clave pública del LAKAUT AC que emitió el certificado.
Identificador de la clave del suscriptor (Subject Key Identifier)	Contiene un hash de 20 bytes del atributo clave pública del suscriptor.
Restricciones básicas (Basic Constraints)	Define el certificado como de entidad final
Uso de claves (Key Usage)	digitalSignature, nonRepudiation, keyEncipherment dataEncipherment,
Uso Extendido de Clave (Extended Key Usage)	Autenticación del cliente, Correo seguro, MS Firma Documento

Política de Certificación (Certificate Policies)	OID 2.16.32.1.1.5 de la Política de Certificación de LAKAUT S.A,y texto obligatorio “certificado emitido por un certificador licenciado en el marco de la Ley Nº 25.506”. CRÍTICA.
Puntos de Distribución de la Lista de Certificados Revocados (CRLDistributionPoints)	URL=https://www.lakautac.com.ar/firma-digital/listadoRevocados
Acceso Información Emisor (Authority Information Access)	CA Issuer: URI https://www.lakautac.com.ar/crt/lakautac.crt OCSP: https://www.lakautac.com.ar/crl/lakautac.ocsp/ CA Issuer: URI https://www.lakautac.com.ar/crt/lakautac.crt OCSP: https://www.lakautac.com.ar/crl/lakautac.ocsp/
Nombres Alternativos del Suscriptor (Subject Alternative Name)	Nombres Alternativos del Suscriptor (Subject Alternative Name)

B) Los siguientes campos se encuentran presentes en los certificados emitidos a **personas jurídicas** por la **AC – LAKAUT**:

Certificado X.509 v3 Atributos / Extensiones	**Contenido**
Versión (Versión)	Valor 2 que corresponde a Versión 3
Número de serie (SerialNumber)	Entero positivo asignado unívocamente por la AC-LAKAUT a cada certificado
Algoritmo de Firma (SignatureAlgoritm)	Algoritmo usado por el certificador para firmar. Puede ser SHA-1.

Nombre distintivo del emisor (Issuer DN)	CN = AC-LAKAUT SERIALNUMBER = CUIT 30710964277 O = LAKAUT S.A. S = Ciudad Autónoma de Buenos Aires C = AR
Validez (desde, hasta) (Valid From / Valid To)	2 años
Nombre distintivo del suscriptor (Subject DN)	CN = Nombre de la unidad operativa responsable del servicio. O = Nombre de la Persona Jurídica Pública o Privada. OU = (Opcional) Las unidades operativas relacionadas con el suscriptor. SERIALNUMBER = Tipo y número de identificación de la Persona Jurídica. Debiendo respetar el formato CUIT y el número de CUIT de la Persona Jurídica. C = AR T= Cargo o título del suscriptor dentro de la organización, debe corresponder con la certificación aportada en el proceso
Clave pública del suscriptor (Subject Public Key Info)	Tipo de algoritmo: RSA Longitud de clave: 2048 Bits
Extensiones	
Identificador de la clave de la Autoridad Certificante (Authority Key Identifier)	Contiene un hash de 20 bytes del atributo clave pública del LAKAUT AC que emitió el certificado.
Identificador de la clave del suscriptor (Subject Key dentifier)	Contiene un hash de 20 bytes del atributo clave pública del suscriptor
Restricciones básicas (Basic Constraints)	Define el certificado como de entidad final
Uso de claves (Key Usage)	digitalSignature, nonRepudiation, keyEncipherment dataEncipherment,

Uso Extendido de Clave (Extended Key Usage)	Autenticación del cliente, Correo seguro
Política de Certificación (Certificate Policies)	OID 2.16.32.1.1.5 de la Política de Certificación de LAKAUT S.A, https://www.lakautac.com.ar/cps.pdf de la Política de Certificación y texto obligatorio “certificado emitido por un certificador licenciado en el marco de la Ley Nº 25.506”. CRÍTICA
Puntos de Distribución de la Lista de Certificados Revocados (CRLDistributionPoints)	URI=http://www.lakautac.com.ar/crl/lakautac.crl
Acceso Información Emisor (Authority Information Access)	CA Issuer: URI https://www.lakautac.com.ar/crt/lakautac.crt OCSP: https://www.lakautac.com.ar/crl/lakautac.ocsp/
Nombres Alternativos del Suscriptor (Subject Alternative Name)	CN = Nombre que figura en el Documento de Identidad del responsable de certificado. SERIALNUMBER = Tipo y número de identificación del Alternativos del Suscriptor (Subject Alternative Name) titular o de documento. “[CUIT/CUIL] [número] T = Cargo o título del suscriptor dentro de la organización, debe corresponder con la certificación aportada en el proceso de autenticación RFC822 = Dirección de mail del suscriptor

C) Los siguientes campos se encuentran presentes en los certificados emitidos a

aplicaciones por la **AC – LAKAUT**:

Certificado X.509 v3 Atributos / Extensiones	Contenido
Versión (Versión)	Valor 2 que corresponde a Versión 3
Número de serie (SerialNumber)	Entero positivo asignado unívocamente por la AC-LAKAUT a cada certificado
Algoritmo de Firma (SignatureAlgoritm)	Algoritmo usado por el certificador para firmar. Puede ser SHA-1.
Nombre distintivo del emisor (Issuer DN)	CN = AC-LAKAUT SERIALNUMBER = CUIT 30710964277 O = LAKAUT S.A. S = Ciudad Autónoma de Buenos Aires C = AR
Validez (desde, hasta) (Valid From / Valid To)	2 años
Nombre distintivo del suscriptor (Subject DN)	CN = Unidad operativa responsable del servicio o aplicación. SERIALNUMBER = Tipo y número de identificación de la Persona Jurídica. Debiendo respetar el formato CUIT y el número de CUIT de la Persona Jurídica. OU = (Opcional) Las unidades operativas relacionadas con el suscriptor. O = Nombre de la Persona Jurídica responsable de la aplicación. C = AR
Clave pública del suscriptor (Subject Public Key Info)	Tipo de algoritmo: RSA Longitud de clave: 2048 Bits
Extensiones	
Identificador de la clave de la Autoridad Certificante (Authority Key Identifier)	Contiene un hash de 20 bytes del atributo clave pública del LAKAUT AC que emitió el certificado.

Identificador de la clave del suscriptor (Subject Key Identifier)	Contiene un hash de 20 bytes del atributo clave pública del suscriptor
Restricciones básicas (Basic Constraints)	Define el certificado como de entidad final
Uso de claves (Key Usage)	digitalSignature, nonRepudiation, keyEncipherment dataEncipherment, contentCommitment, keyAgreement, encipherOnly, decipherOnly
Uso Extendido de Clave (Extended Key Usage)	Autenticación del cliente, Autenticación del servidor
Política de Certificación (Certificate Policies)	OID de la Política de Certificación de LAKAUT S.A, URI de la Política de Certificación y texto obligatorio “certificado emitido por un certificador licenciado en el marco de la Ley Nº 25.506”. CRÍTICA
Puntos de Distribución de la Lista de Certificados Revocados (CRLDistributionPoints)	URI=http://www.lakautac.com.ar/crl/lakautac.crl
Acceso Información Emisor (Authority Information Access)	CA Issuer: URI https://www.lakautac.com.ar/crt/lakautac.crt OCSP: https://www.lakautac.com.ar/crl/lakautac.ocsp/
Nombres Alternativos del Suscriptor (Subject Alternative Name)	CN = Nombre que figura en el Documento de Identidad del responsable de certificado. SERIALNUMBER = Tipo y número de identificación del titular o de documento. “[CUIT/CUIL] [número] T = Cargo o título del suscriptor dentro de la organización, debe corresponder con la certificación aportada en el proceso de autenticación RFC822 = Dirección de mail del suscriptor

D) Los siguientes campos se encuentran presentes en los certificados emitidos a **sitios seguros** por la **AC – LAKAUT**:

Certificado X.509 v3 Atributos / Extensiones	**Contenido**
Versión (Versión)	Valor 2 que corresponde a Versión 3
Número de serie (Serial Number)	Entero positivo asignado unívocamente por la AC-LAKAUT a cada certificado
Algoritmo de Firma (SignatureAlgoritm)	Algoritmo usado por el certificador para firmar. Puede ser SHA-1.
Nombre distintivo del emisor (Issuer DN)	CN = AC-LAKAUT SERIALNUMBER = CUIT 30710964277 O = LAKAUT S.A. S = Ciudad Autónoma de Buenos Aires C = AR
Validez (desde, hasta) (Valid From / Valid To)	2 años
Nombre distintivo del suscriptor (Subject DN)	CN = Denominación del sitio web de Internet. OU = (Opcional) Las unidades operativas relacionadas con el sitio seguro. O = Nombre de la Persona Jurídica responsable del sitio. SERIALNUMBER = Tipo y número de identificación de la Persona Jurídica. Debiendo respetar el formato CUIT y el número de CUIT de la Persona Jurídica. C = AR
Clave pública del suscriptor (Subject Public Key Info)	Tipo de algoritmo: RSA Longitud de clave: 2048 Bits
Extensiones	
Identificador de la clave de la Autoridad Certificante	Contiene un hash de 20 bytes del atributo clave pública del LAKAUT AC que emitió el certificado.

(Authority Key Identifier)	
Identificador de la clave del suscriptor (Subject Key Identifier)	Contiene un hash de 20 bytes del atributo clave pública del suscriptor
Restricciones básicas (Basic Constraints)	Define el certificado como de entidad final
Uso de claves (Key Usage)	digitalSignature, nonRepudiation, keyEncipherment dataEncipherment, contentCommitment, keyAgreement,
Uso Extendido de Clave (Extended Key Usage)	Autenticación del cliente, Autenticación del servidor
Política de Certificación (Certificate Policies)	OID de la Política de Certificación de LAKAUT S.A, URI de la Política de Certificación y texto obligatorio “certificado emitido por un certificador licenciado en el marco de la Ley Nº 25.506”. CRÍTICA
Puntos de Distribución de la Lista de Certificados Revocados (CRLDistributionPoints)	URI=http://www.lakautac.com.ar/crl/lakautac.crl
Acceso Información Emisor (Authority Information Access)	CA Issuer: URI https://www.lakautac.com.ar/crt/lakautac.crt OCSP: https://www.lakautac.com.ar/crl/lakautac.ocsp/

Nombres Alternativos del Suscriptor (Subject Alternative Name)	CN = Nombre que figura en el Documento de Identidad del responsable de certificado. SERIALNUMBER = Tipo y número de identificación del titular o de documento. “[CUIT/CUIL] [número] T = Cargo o título del suscriptor dentro de la organización, debe corresponder con la certificación aportada en el proceso de autenticación RFC822 = Dirección de mail del suscriptor

E) Los siguientes campos se encuentran presentes en los **Certificados de Autoridad de Sello de tiempo**:

Certificado X.509 v3 Atributos / Extensiones	**Contenido**
Versión (Versión)	Valor 2 que corresponde a Versión 3
Número de serie (Serial Number)	Entero positivo asignado unívocamente por la AC-LAKAUT a cada certificado
Algoritmo de Firma (SignatureAlgorithm)	Algoritmo usado por el certificador para firmar. Puede ser SHA-1.
Nombre distintivo del emisor (Issuer DN)	CN = AC-LAKAUT SERIALNUMBER = CUIT 30710964277 O = LAKAUT S.A. S = Ciudad Autónoma de Buenos Aires C = AR
Validez (desde, hasta) (Valid From / Valid To)	2 años
Nombre distintivo del suscriptor (Subject DN)	CN = Denominación del sitio web de Internet. OU = (Opcional) Las unidades operativas relacionadas con el sitio seguro. O = Nombre de la Persona Jurídica responsable del sitio. SERIALNUMBER = Tipo y número de identificación de la Persona Jurídica. Debiendo respetar el formato CUIT y el número de CUIT de la Persona Jurídica. C = AR

Clave pública del suscriptor (Subject Public Key Info)	Tipo de algoritmo: RSA Longitud de clave: 2048 Bits
Extensiones	
Identificador de la clave de la Autoridad Certificante (Authority Key Identifier)	Contiene un hash de 20 bytes del atributo clave pública del LAKAUT AC que emitió el certificado.
Identificador de la clave del suscriptor (Subject Key Identifier)	Contiene un hash de 20 bytes del atributo clave pública del suscriptor
Restricciones básicas (Basic Constraints)	CA = FALSE Pathlen = 0
Uso de claves (Key Usage)	digitalSignature, nonRepudiation, keyEncipherment dataEncipherment, contentCommitment, keyAgreement,
Uso Extendido de Clave (Extended Key Usage)	Time Stamping (1.3.6.1.5.5.7.3.8)
Política de Certificación (Certificate Policies)	OID 2.16.32.1.1.5 de la Política de Certificación de LAKAUT S.A. https://www.lakautac.com.ar/cDS.Ddf de la Política de Certificación y texto obligatorio “certificado emitido por un certificador licenciado en el marco de la Ley N° 25.506”. CRÍTICA.
Puntos de Distribución de la Lista de Certificados Revocados (CRLDistributionPoin	URI=http://www.lakautac.com.ar/crl/lakautac.crl

ts)	
Acceso Información Emisor (Authority Information Access)	CA Issuer: URI https://www.lakautac.com.ar/crt/lakautac.crt OCSP: https://www.lakautac.com.ar/crl/lakautac.ocsp/

F) Perfil de Certificados de **Autoridad de sello de competencia:**

Certificado X.509 v3 Atributos / Extensiones	**Contenido**
Versión (Versión)	Valor 2 que corresponde a Versión 3
Número de serie (SerialNumber)	Entero positivo asignado unívocamente por la AC-LAKAUT a cada certificado
Algoritmo de Firma (SignatureAlgoritm)	Algoritmo usado por el certificador para firmar. es SHA-1.
Nombre distintivo del emisor (Issuer DN)	CN = AC-LAKAUT SERIALNUMBER = CUIT 30710964277 O = LAKAUT S.A. S = Ciudad Autónoma de Buenos Aires C = AR
Validez (desde, hasta) (Valid From / Valid To)	2 años
Nombre distintivo del suscriptor (Subject DN)	CN = Nombre de la unidad operativa responsable del servicio. O = Nombre de la Persona Jurídica Pública o Privada. OU = (Opcional) Las unidades operativas relacionadas con el suscriptor. SERIALNUMBER = Tipo y número de identificación de la Persona Jurídica. Debiendo respetar el formato CUIT y el número de CUIT de la Persona Jurídica. C = AR T= Cargo o título del suscriptor dentro de la organización, debe corresponder con la certificación aportada en el proceso

Clave pública del suscriptor (Subject Public Key Info)	Tipo de algoritmo: RSA Longitud de clave: 2048 Bits
Extensiones	
Identificador de la clave de la Autoridad Certificante (Authority Key Identifier)	Contiene un hash de 20 bytes del atributo clave pública del LAKAUT AC que emitió el certificado.
Identificador de la clave del suscriptor (Subject Key dentifier)	Contiene un hash de 20 bytes del atributo clave pública del suscriptor
Restricciones básicas (Basic Constraints)	Define el certificado como de entidad final
Uso de claves (Key Usage)	digitalSignature, nonRepudiation, keyEncipherment dataEncipherment,
Uso Extendido de Clave (Extended Key Usage)	Autenticación del cliente, Correo seguro
Política de Certificación (Certificate Policies)	OID 2.16.32.1.1.5 de la Política de Certificación de LAKAUT S.A, https://www.lakautac.com.ar/cps.pdf de la Política de Certificación y texto obligatorio “certificado emitido por un certificador licenciado en el marco de la Ley Nº 25.506”. CRÍTICA
Puntos de Distribución de la Lista de Certificados Revocados (CRLDistributionPoints)	URI=http://www.lakautac.com.ar/crl/lakautac.crl
Acceso Información Emisor	CA Issuer: URI https://www.lakautac.com.ar/crt/lakautac.crt

(Authority Information Access)	OCSP: https://www.lakautac.com.ar/crl/lakautac.ocsp/
Nombres Alternativos del Suscriptor (Subject Alternative Name)	CN = Nombre que figura en el Documento de Identidad del responsable de certificado. SERIALNUMBER = Tipo y número de identificación del Alternativos del Suscriptor (Subject Alternative Name) titular o de documento. “[CUIT/CUIL] [número] T = Cargo o título del suscriptor dentro de la organización, debe corresponder con la certificación aportada en el proceso de autenticación RFC822 = Dirección de mail del suscriptor

7.2 - Perfil de la lista de certificados revocados.

Las listas de certificados revocados correspondientes a la presente Política de Certificación son emitidas conforme con lo establecido en la especificación ITU

X.509 versión 2 o la que en su defecto, determine la Secretaría de Innovación Pública, y cumplirán con las indicaciones establecidas en el apartado “3- Perfil de CRLs” del Anexo IV – “Perfiles de los Certificados y de las Listas de Certificados Revocados”. Mediente la URL de acceso: https://www.lakautac.com.ar/crl/lakautac.crl

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

La consulta en línea del estado de un certificado digital se realiza utilizando el Protocolo OCSP (Online Certifícate Status Protocol). Deberá ser implementada conforme a lo indicado en la especificación RFC 6960 y cumplir con las indicaciones establecidas en la apartado 4 - Perfil de la consulta en línea del estado del certificado” del Anexo IV - “Perfiles de los Certificados y de las Listas de Certificados Revocados”. Según Resolución 946/2021 de la entonces Secretaría de Innovación Pública de la JEFATURA DE GABINETE DE MINISTROS.

7.3.1. – Consultas OCSP

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

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

7.3.2. - Respuestas OCSP

Las características operacionales del servicio se encuentran disponibles en el sitio web de Lakaut AC.
El acceso al servicio OCSP permite, mediante su consulta, determinar el estado de validez de un certificado digital y es provisto ingresando con su Usuario y Password en el sitio Web.: https://www.lakautac.com.ar/firma-digital/listadoRevocados

8 – AUDITORÍA DE CUMPLIMIENTO Y OTRAS EVALUACIONES.

El certificador LAKAUT, se encuentra sujeto a las auditorías dispuestas en el artículo 10 del Decreto N° 561/16 de fecha 6 de abril de 2016.

Asimismo, se encuentra sujeta a inspecciones extraordinarias realizadas u ordenadas por la Secretaría de Innovación Pública, en cumplimiento del Anexo II, Sección 2 de la Resolución 946/2021.

Los aspectos a evaluar se encuentran establecidos en el artículo 3 de la Ley N° 27.446 y otras normas reglamentarias.

Los informes resultantes de las auditorías son elevados a la Secretaría de Innovación Pública. Las fechas son publicadas en el sitio web.de la AC - LAKAUT: https://www.lakautac.com.ar

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

Se cumplen las exigencias reglamentarias impuestas por:

a) El artículo 33 de la Ley N° 25.506 de Firma Digital, respecto al sistema de auditoría y el artículo 21, inciso k) de la misma Ley, relativo a la publicación de informes de auditoría.

b) El artículo 6° del Anexo al Decreto Nº 182/2019 relativo al sistema de auditoría y el artículo 7° del mismo decreto relativo al informe de auditoría.

9 – ASPECTOS LEGALES Y ADMINISTRATIVOS.

9.1 – Aranceles.

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

Los aranceles para las distintas clases de certificados serán publicados en el siguiente sitio web de **LAKAUT S.A**.:

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

9.2 - Responsabilidad Financiera.

La responsabilidad financiera se origina en lo establecido por la Ley Nº 25.506 y su Decreto Reglamentario Nº182/2019 y en las disposiciones de la presente política.

La AC Lakaut constituye una garantía mediante un seguro de caución a fin de garantizar el cumplimiento de sus obligaciones de lo establecido por el Artículo 41 Anexo I, de la Resolución 946/2021 de la entonces Secretaría de Innovación Pública de la JEFATURA DE GABINETE DE MINISTROS.

9.3 – Confidencialidad.

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

Se especifica la información a ser tratada como confidencial por el certificador y por las Autoridades de Registro operativamente vinculadas, de acuerdo con lo establecido por las

normas legales y reglamentarias vigentes.

9.3.1 - Información confidencial

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

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

LAKAUT S.A., en su carácter de Certificador, garantiza la confidencialidad frente a terceros de su clave privada, la que, al ser el punto de máxima confianza, será generada y custodiada conforme a lo que se especifica 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 transmita 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.
- Es considerada confidencial la información incluida en el Manual de Procedimientos de Seguridad y en el Plan de Contingencia de la **AC – LAKAUT**.

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

9.3.2 - Información no confidencial.

La siguiente información recibida por la AC Lakut y sus AR no se considera confidencial:

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

b) Información sobre personas humanas o jurídicas que se encuentre disponible

en certificados o en directorios de acceso público.

c) Política Únicas de Certificación y Manual de Procedimientos.

d) Secciones públicas del Plan de Seguridad del Certificador.

e) Política de privacidad del Certificador.

f) Acuerdo con suscriptores.

g) Términos y condiciones con terceros usuarios.

9.3.3 - Responsabilidades de los roles involucrados.

Describe las responsabilidades de los roles que gestionan información confidencial en cuanto a evitar su compromiso o divulgación a personas no autorizadas

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

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, pasaporte, documento de identidad expedido por país miembro del MERCOSUR u ocupación.
- Aquellos para los que el Certificador hubiera obtenido autorización expresa de su titular.

9.4 – Privacidad

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

9.5 - Derechos de Propiedad Intelectual

Las aplicaciones y los sistemas informáticos generados por el Certificador con el objeto de desarrollar e implementar la **AC – LAKAUT** son propiedad de **LAKAUT S.A.**

Los sistemas operativos y de soporte informático no desarrollados por **LAKAUT S.A.** cuentan con su respectiva licencia de uso.

Los datos propios de la **AC – LAKAUT** incluidos en esta Política Única de Certificación son de propiedad de **LAKAUT S.A.**

9.6 – Responsabilidades y garantías.

Se regirá por lo establecido en la Ley N° 25.506, su decreto reglamentario N° 182/19, Resolución 946/2021 de la entonces Secretaría de Innovación Pública de la JEFATURA DE GABINETE DE MINISTROS y toda otra Resolución que emita sobre esta materia la Secretaría de Innovación Pública dependiente de JEFATURA DE GABINETE DE MINISTROS.

Las partes contratantes se rigen además por el Acuerdo con Suscriptores que es el contrato específico que regula la relación entre el suscriptor y el Certificador Licenciado LAKAUT S.A.

9.7 – Deslinde de responsabilidad.

Las limitaciones de responsabilidad de la AC se rigen por lo establecido en el artículo 39 de la Ley N° 25.506, en las disposiciones de la presente política y en el Acuerdo con Suscriptores.

9.8 – Limitaciones a la responsabilidad frente a terceros.

Las limitaciones de responsabilidad de la AC respecto a otras entidades participantes, se rigen por lo establecido en el artículo 39 de la Ley N° 25.506, en las disposiciones de la presente política y en los términos y condiciones con terceros usuarios, establecidos en el Acuerdo con Suscriptores firmado por los suscriptores con el Certificador Licenciado.

También aplica la limitación impuesta en casos de fuerza mayor conforme la definición establecida en el Código Civil y Comercial Unificado.

9.9 – Compensaciones por daños y perjuicios.

No aplica.

9.10 - Condiciones de vigencia.

La presente Política Única empieza a ser efectiva una vez que el acto administrativo por el cual la autoridad competente la aprueba sea publicado en el BORA.

A partir de dicha publicación los nuevos certificados serán emitidos cumplimiento las políticas determinadas en la nueva versión.

La Política Única de Certificación estará en vigor mientras no sea derogada y reemplazada por una nueva versión.

9.11 - Avisos personales y comunicaciones con los participantes.

No aplicable.

9.12 - Gestión del ciclo de vida del documento.

Si el responsable del documento definido en el punto 1.5.1 de la presente PUC considerara pertinente la modificación del documento deberá someter a consideración y evaluación del Certificador Licenciado **LAKAUT S.A.** las correspondientes propuestas.

Si los cambios o modificaciones propuestas son aceptados, por LAKAUT AC esta lo deberá presentar para su aprobación ante Secretaría de Innovación Pública dependiente de JEFATURA DE GABINETE DE MINISTRO, y tendrán como resultado final la aprobación de una nueva versión de la Política Única de Certificación.

9.12.1 - Procedimientos de cambio.

Las modificaciones a la presente Política Única de Certificación, deberán ser aprobadas previamente por la Secretaría de Innovación Pública dependiente de JEFATURA DE GABINETE DE MINISTROS, conforme a lo establecido por la Ley N° 25.506, artículo 21, inciso q), por la Resolución 946/2021 de la entonces Secretaría de Innovación Pública de la JEFATURA DE GABINETE DE MINISTROS y sus anexos respectivos.

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

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

9.12.2 – Mecanismo y plazo de publicación y notificación.

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

Una vez que la Autoridad de Aplicación notifique al Certificador la aprobación de las modificaciones a la Política de Certificación, éste procederá a su publicación en el sitio web antes mencionado.

9.12.3 – Condiciones de modificación del OID.

No aplicable.

9.13 - Procedimientos de resolución de conflictos.

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 **AC - LAKAUT**.
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.

El Certificador Licenciado resolverá en un plazo de DIEZ (10) días lo que estime corresponder, 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 vigente de firma digital.

El suscriptor o los terceros usuarios podrán accionar ante la Secretaría de Innovación Pública dependiente de JEFATURA DE GABINETE DE MINISTRO, previo
agotamiento del procedimiento ante **AC - LAKAUT**, el cual deberá proveer obligatoriamente al interesado de un adecuado procedimiento de resolución de conflictos.

9.14 - Legislación aplicable.

La legislación que respalda la interpretación, aplicación y validez de la Política Única de Certificación, es la Ley Nº 25.506, el Decreto Nº 182/2019, y toda otra norma complementaria dictada por la autoridad competente.

9.15 – Conformidad con normas aplicables.

La legislación aplicable a la actividad del Certificador es la Ley N° 25.506, el Decreto Reglamentario N° 182/2019, la Resolución 946/2021 de la entonces Secretaría de Innovación Pública de la JEFATURA DE GABINETE DE MINISTROS y toda otra norma complementaria dictada por la autoridad competente.

9.16 – Cláusulas adicionales.

No se establecen cláusulas adicionales.

9.17 – Otras cuestiones general

No aplicable.

Historial de revisión:

VERSIÓN Y MODIFICACIÓN	EMISIÓN	DESCRIPCIÓN	MOTIVO DEL CAMBIO
Versión 1.0	15 de mayo de 2015	Política Única de Certificación (PUC)	Licenciamiento **AC - LAKAUT**
Versión 2.0	2021	Política Única de Certificación (PUC)	Renovación de la licencia **AC - LAKAUT**

Nota: Cada nueva versión y/o modificación suplanta a las anteriores, resultando sólo vigente la última, la que está representada por el presente documento.

República Argentina - Poder Ejecutivo Nacional
Las Malvinas son argentinas

Hoja Adicional de Firmas
Anexo

Número: IF-2022-91402627-APN-SSIA#JGM

CIUDAD DE BUENOS AIRES
Miércoles 31 de Agosto de 2022

Referencia: Política Única de Certificación V.2. - LAKAUT S.A.

El documento fue importado por el sistema GEDO con un total de 90 pagina/s.

Digitally signed by Gestion Documental Electronica
Date: 2022.08.31 11:19:44 -03:00

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

Digitally signed by Gestion Documental Electronica
Date: 2022.08.31 11:19:45 -03:00