Política Única de Certificación

Jacobs Comercial S.R.L. (Egregor Labs) — Versión 1.1 — Fecha: [●] — Clase: Público

Versiones y modificaciones de este documento

Versión	Fecha	Elaborado por	Revisado por	Descripción
1.0	[●]	Responsable de la AC	Gerencia	Versión inicial para el licenciamiento
1.1	7/11/2026	Responsable de la AC	Gerencia	Razón social Jacobs Comercial S.R.L., nombre de fantasía Egregor Labs, aplicación Advanced Electronic Signature (AdES), domicilio y CUIT

1. Introducción

1.1. Descripción general

El presente documento establece las políticas que se aplican a la relación entre Jacobs Comercial S.R.L., que gira bajo el nombre de fantasía “Egregor Labs” (en adelante, indistintamente, “Jacobs Comercial S.R.L.”, “Egregor Labs” o “el Certificador”), cuya Autoridad Certificante se denomina “AC EGREGOR”, en su carácter de certificador licenciado, y los solicitantes, suscriptores y terceros usuarios de los certificados que emita, en el marco de la Infraestructura de Firma Digital de la República Argentina (Ley N° 25.506 y su modificatoria, Decreto N° 182/2019 y sus modificatorios, Decreto N° 743/2024, Resolución SICYT N° 11/2025 y toda otra norma complementaria dictada por la autoridad competente). Un certificado vincula los datos de verificación de firma digital de una persona humana o jurídica a un conjunto de datos que permiten identificarla, conocida como suscriptor del certificado.

Jacobs Comercial S.R.L. es la sociedad que contrata con los solicitantes y suscriptores y que presta todos los servicios descriptos en esta Política. “Egregor Labs” es únicamente su nombre de fantasía y no constituye una persona distinta. La aplicación con la que se prestan los servicios se denomina “Advanced Electronic Signature” (en adelante, “AdES”).

Egregor Labs emite certificados de firma digital para personas humanas y para personas jurídicas públicas o privadas. Los pares de claves de los suscriptores se generan y se guardan en el módulo criptográfico integrado al teléfono del suscriptor (Secure Enclave de los dispositivos Apple iPhone), mediante la aplicación habilitada AdES. La clave privada no puede exportarse del módulo, y cada uso exige, en el propio dispositivo, la autenticación biométrica de su titular y su contraseña de firma. La identidad de los solicitantes se valida con el servicio de validación de identidad del Registro Nacional de las Personas (RENAPER), en forma remota o presencial.

La Autoridad de Aplicación de la Infraestructura de Firma Digital es la Secretaría de Innovación, Ciencia y Tecnología de la Jefatura de Gabinete de Ministros. Dicho organismo y la Subsecretaría de Innovación ejercen las funciones de Ente Licenciante. El certificado de la AC EGREGOR es emitido por la Autoridad Certificante Raíz de la República Argentina (AC-RAÍZ).

1.2. Nombre e identificación del documento

Nombre	Política Única de Certificación de Jacobs Comercial S.R.L. (Egregor Labs)
Versión	1.1
Fecha de aplicación	[fecha del acto administrativo aprobatorio]
OID	[OID asignado por la Dirección Nacional de Firma Digital e Infraestructura Tecnológica]
URL	https://advancedelectronicsignature.com/politicas/puc.pdf
Lugar	República Argentina

1.3. Participantes

Integran la infraestructura del Certificador las siguientes entidades.

1.3.1. Certificador

Razón social	Jacobs Comercial S.R.L.
Nombre de fantasía	Egregor Labs
CUIT	30-71902710-1
Domicilio	Cabello 3352, piso 3 (C1425), Ciudad Autónoma de Buenos Aires, República Argentina
Correo electrónico	[●]@advancedelectronicsignature.com
Teléfono	[●]
Sitio web	https://advancedelectronicsignature.com
Aplicación habilitada	Advanced Electronic Signature (AdES)

1.3.2. Autoridad de Registro

Egregor Labs opera una única Autoridad de Registro, la Autoridad de Registro Central (AR CENTRAL), que recibe las solicitudes de emisión, valida la identidad de los solicitantes, procesa las renovaciones y recibe y valida las solicitudes de revocación. La AR CENTRAL actúa en dos modalidades:

- **Modalidad remota (presencia telemática):** la solicitud se tramita desde la aplicación habilitada AdES. La identidad se valida con la captura del rostro del solicitante y su cotejo en tiempo real con el RENAPER, conforme al Decreto N° 743/2024.
- **Modalidad presencial:** la solicitud se tramita ante un Oficial de Registro, en el domicilio de la AR CENTRAL, con captura de rostro y huellas dactilares y cotejo con el RENAPER. Se usa a elección del solicitante y como contingencia según el punto 3.2.4.

Contacto	Responsable de la Autoridad de Registro Central

Domicilio	Cabello 3352, piso 3 (C1425), Ciudad Autónoma de Buenos Aires
Correo electrónico	ar@advancedelectronicsignature.com
Teléfono	[●]
Sitio web	https://advancedelectronicsignature.com/autoridad-de-registro

El listado actualizado de Autoridades de Registro se publica conforme al punto 2.3. Egregor Labs no opera Autoridades de Registro en modalidad móvil.

1.3.3. Suscriptores de certificados

Son suscriptores de los certificados emitidos bajo esta Política:

- **Personas humanas** mayores de edad que cuenten con Documento Nacional de Identidad (DNI) y CUIL o CUIT, y con un dispositivo compatible según el punto 6.2.11. Los extranjeros deben contar con DNI argentino, ya que la validación de identidad se realiza contra el RENAPER.
- **Personas jurídicas públicas o privadas** con CUIT, que solicitan el certificado por medio de su representante legal o de un apoderado con poder suficiente. Esa persona humana es la responsable de la custodia de la clave privada, que se genera en su dispositivo compatible.

Egregor Labs no emite certificados de aplicaciones, de sitio seguro, de Autoridad de Sello de Tiempo ni de Autoridad de Sello de Competencia, y no presta el servicio de firma digital con custodia centralizada de claves.

Jacobs Comercial S.R.L. es suscriptora de un certificado emitido por su propia Autoridad Certificante para firmar las respuestas del servicio OCSP.

1.3.4. Terceros usuarios

Son terceros usuarios de los certificados emitidos bajo esta Política toda persona humana o jurídica que recibe un documento firmado digitalmente y que genera una consulta para verificar la validez del certificado digital correspondiente, de acuerdo con la normativa vigente.

1.4. Uso de los certificados

Las claves correspondientes a los certificados emitidos bajo esta Política pueden ser utilizadas por sus titulares en forma interoperable para firmar digitalmente cualquier documento o transacción, y para autenticación o cifrado.

Por tratarse de claves de curva elíptica, el cifrado se realiza mediante esquemas de acuerdo de claves (por ejemplo, ECIES), que el módulo criptográfico del dispositivo ejecuta con la misma autenticación que la firma (biometría y contraseña de firma). La pérdida del control de la clave privada impide descifrar los datos cifrados para ella. Los certificados no pueden usarse para fines contrarios a la ley ni fuera de los límites del punto 4.5.

1.5. Administración de la Política

1.5.1. Organización administradora del documento

Organización	Jacobs Comercial S.R.L. (Egregor Labs)
Servicio de atención de consultas	Mesa de Ayuda de Egregor Labs
Correo electrónico institucional	ayuda@advancedelectronicsignature.com
Teléfono	[●]

1.5.2. Contacto

El responsable del registro, mantenimiento e interpretación de esta Política es el Responsable de la Autoridad Certificante de Egregor Labs.

Contacto	Responsable de la Autoridad Certificante
Domicilio	Cabello 3352, piso 3 (C1425), Ciudad Autónoma de Buenos Aires
Correo electrónico	ac@advancedelectronicsignature.com
Teléfono	[●]

1.5.3. Organismo encargado de aprobar la Política Única de Certificación

Esta Política fue presentada ante el Ente Licenciante durante el proceso de licenciamiento, de conformidad con la Ley N° 25.506, el Decreto N° 182/2019 y modificatorios y la Resolución SICYT N° 11/2025, y fue aprobada mediante el correspondiente acto administrativo [●].

1.6. Definiciones y acrónimos

1.6.1. Definiciones

AdES: abreviatura de “Advanced Electronic Signature”, nombre de la aplicación habilitada.

Aplicación habilitada: la aplicación móvil “Advanced Electronic Signature” (“AdES”) para iOS, desarrollada y provista por Jacobs Comercial S.R.L., incluida su extensión “Firmar con AdES” para firmar desde otras aplicaciones, autorizada por Egregor Labs para generar el par de claves del suscriptor en el módulo criptográfico del dispositivo, armar la solicitud de certificado, capturar el rostro del solicitante, obtener la atestación de la aplicación, recibir el certificado, firmar documentos y solicitar la revocación.

Atestación de la aplicación: evidencia criptográfica emitida por el servicio App Attest de Apple, que acredita que una solicitud proviene de una instancia de la aplicación habilitada, identificada por el equipo de desarrollo y el identificador de la aplicación registrados ante Apple, ejecutada en un dispositivo Apple genuino.

Autoridad de Aplicación: la Secretaría de Innovación, Ciencia y Tecnología de la Jefatura de Gabinete de Ministros, que dicta las normas reglamentarias de aplicación de la Ley N° 25.506 y la normativa regulatoria de firma digital de la República Argentina.

Autoridad de Registro: entidad que tiene a su cargo las siguientes funciones, delegadas por el Certificador Licenciado: (a) recepción de las solicitudes de emisión de certificados; (b) validación de la identidad y autenticación de los datos de los titulares de certificados; (c) validación de otros datos de los titulares de certificados que se presenten ante ella y cuya verificación delegue el Certificador Licenciado; (d) remisión de las solicitudes aprobadas al Certificador Licenciado con el que se encuentre operativamente vinculada; (e) recepción y validación de las solicitudes de revocación de certificados y su direccionamiento al Certificador Licenciado; (f) identificación y autenticación de los solicitantes de revocación de certificados; (g) archivo y conservación de toda la documentación de respaldo del proceso de validación de identidad, de acuerdo con los procedimientos establecidos por el Certificador Licenciado; (h) cumplimiento de las normas y recaudos establecidos para la protección de datos personales; e (i) cumplimiento de las disposiciones de esta Política y del Manual de Procedimientos, en la parte que resulte aplicable.

Autoridad de Sello de Competencia: entidad que acredita competencias, roles, funciones o relaciones laborales del titular de un certificado de firma digital.

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.

Certificado digital: 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: toda persona de existencia ideal, registro público de contratos u organismo público que expide certificados, presta otros servicios en relación con la firma digital y cuenta con una licencia para ello, otorgada por el Ente Licenciante (artículo 17 de la Ley N° 25.506). A los efectos de esta Política, Jacobs Comercial S.R.L.

Contraseña de firma: contraseña que el suscriptor define en la aplicación habilitada al generar su par de claves y que el módulo criptográfico del dispositivo exige, junto con la biometría, en cada uso de la clave privada. Es distinta de la contraseña de la cuenta.

Cuenta: registro del usuario en la aplicación habilitada, al que se accede con email y contraseña o con una cuenta de Apple, Google o Microsoft. La cuenta no acredita la identidad del titular, que se valida siempre conforme al punto 3.2.3.

Dispositivo compatible: teléfono Apple iPhone cuyo módulo criptográfico cumple los requisitos del punto 6.2.11 para la versión de sistema operativo instalada.

Egregor Labs: nombre de fantasía de Jacobs Comercial S.R.L. Toda mención a Egregor Labs en esta Política y en los documentos que la complementan se refiere a Jacobs Comercial S.R.L.

Ente Licenciante: la Secretaría de Innovación, Ciencia y Tecnología y la Subsecretaría de Innovación de la Jefatura de Gabinete de Ministros, encargadas de aprobar las Políticas Únicas de Certificación, el Manual de Procedimientos, el Plan de Seguridad, el Plan de Cese de Actividades y el Plan de Contingencia de los certificadores.

Infraestructura tecnológica del Certificador: conjunto de servidores y otros equipamientos informáticos, software y dispositivos criptográficos utilizados para la generación,

almacenamiento y publicación de los certificados, para la provisión de información sobre su estado de validez y para la prestación de los demás servicios del Certificador. Se sitúa en territorio argentino, tanto en el establecimiento principal como en el de contingencia, bajo el control de Jacobs Comercial S.R.L. y afectada exclusivamente a tareas de certificación.

Lista de certificados revocados (CRL): lista de certificados que han sido dejados sin efecto en forma permanente por el Certificador, firmada digitalmente y publicada por él.

Manual de Procedimientos: conjunto de prácticas utilizadas por el Certificador en la emisión y administración de los certificados (Certification Practice Statement, CPS).

Módulo criptográfico del dispositivo: componente de hardware del teléfono que genera y guarda la clave privada del suscriptor y realiza las operaciones de firma sin permitir la exportación de la clave. En los dispositivos admitidos es el Secure Enclave de Apple.

Frase de confirmación de la revocación: texto "revocar mi certificado" que el suscriptor escribe al pedir la revocación por cualquier vía, con el único fin de confirmar que no lo hace por error.

Plan de Cese de Actividades: conjunto de actividades a desarrollar por el Certificador en caso de finalizar la prestación de sus servicios.

Plan de Contingencia: conjunto de procedimientos a seguir por el Certificador ante situaciones 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.

Política de Privacidad: conjunto de declaraciones que el Certificador se compromete a cumplir para resguardar los datos de los solicitantes y suscriptores de los certificados que emite.

Servicio OCSP: servicio de verificación en línea del estado de los certificados (Online Certificate Status Protocol). Es un método para determinar el estado de revocación de un certificado sin usar la CRL. Sus respuestas están firmadas por el Certificador.

Solicitud de certificado (CSR): requerimiento en formato PKCS#10 que contiene la clave pública y los datos del solicitante, firmado con la clave privada correspondiente.

Suscriptor o titular de certificado digital: persona a cuyo nombre se emite un certificado y que posee una clave privada que se corresponde con la clave pública contenida en él.

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.

1.6.2. Acrónimos

Acrónimo	Significado
AC	Autoridad Certificante
AC-RAÍZ	Autoridad Certificante Raíz de la República Argentina
AdES	Advanced Electronic Signature (nombre de la aplicación habilitada)

Acrónimo	Significado
AR	Autoridad de Registro
ARCA	Agencia de Recaudación y Control Aduanero
CMVP	Cryptographic Module Validation Program (NIST)
CRL	Lista de Certificados Revocados (Certificate Revocation List)
CSR	Solicitud de certificado (Certificate Signing Request, PKCS#10)
CUIL / CUIT	Clave Única de Identificación Laboral / Tributaria
DNFDIT	Dirección Nacional de Firma Digital e Infraestructura Tecnológica
DNI	Documento Nacional de Identidad
ECDSA	Algoritmo de firma digital de curva elíptica
FIPS	Federal Information Processing Standards
HSM	Módulo de seguridad de hardware (Hardware Security Module)
IETF	Internet Engineering Task Force
NIST	National Institute of Standards and Technology
OCSP	Protocolo en línea del estado de un certificado (Online Certificate Status Protocol)
OID	Identificador de objeto (Object Identifier)
OR	Oficial de Registro
RENAPER	Registro Nacional de las Personas
RFC	Request for Comments
SICYT	Secretaría de Innovación, Ciencia y Tecnología
SID	Sistema de Identidad Digital del RENAPER
S.R.L.	Sociedad de Responsabilidad Limitada
SSI	Subsecretaría de Innovación
UTC	Tiempo universal coordinado

2. Responsabilidades vinculadas a la publicación y a los repositorios

Se detallan a continuación las responsabilidades del Certificador respecto del mantenimiento de repositorios, la publicación de certificados y de información sobre sus políticas y procedimientos.

2.1. Repositorios

El repositorio de información y la publicación de la Lista de Certificados Revocados son administrados en forma directa por Egregor Labs, en su infraestructura tecnológica situada en la República Argentina. Egregor Labs no delega en terceros la administración del repositorio. Para mejorar su disponibilidad, puede replicar el contenido público (certificados de la AC y CRL) en una red de distribución de contenidos, sin que ello altere su origen ni su firma.

2.2. Publicación de información del Certificador

Egregor Labs garantiza el acceso a la información actualizada y vigente publicada en su repositorio de los siguientes elementos:

a) Política Única de Certificación vigente y versiones anteriores.
b) Acuerdo con Suscriptores.
c) Términos y Condiciones con Terceros Usuarios.
d) Política de Privacidad.
e) Manual de Procedimientos (parte pública).
f) Información sobre las auditorías e inspecciones que le fueron efectuadas (fecha y organismo que la efectuó).
g) Repositorio de certificados revocados (CRL).
h) Certificado de la AC EGREGOR y acceso al certificado de la AC-RAÍZ.
i) Consulta de certificados emitidos, con indicación de su estado.
j) Listado de Autoridades de Registro.
k) Listado de dispositivos y versiones de sistema operativo admitidos, conforme al punto 6.2.11.

La información se publica en https://advancedelectronicsignature.com/firma-digital. El repositorio está disponible las veinticuatro (24) horas, los siete (7) días de la semana.

2.3. Listado de Autoridades de Registro — Frecuencia de publicación

Egregor Labs garantiza la actualización inmediata del repositorio cada vez que cualquiera de los documentos publicados sea modificado. La CRL se publica con la frecuencia indicada en el punto 4.9.7, y el listado del punto 2.2.k) se actualiza ante cada cambio en el estado de certificación de un módulo criptográfico admitido.

2.4. Controles de acceso a la información

Egregor Labs garantiza los controles de acceso a su certificado, a la Lista de Certificados Revocados y a las versiones anteriores y vigentes de esta Política y del Manual de Procedimientos. Solo el personal autorizado puede modificar el contenido del repositorio, mediante autenticación de doble factor, y cada modificación queda registrada.

Egregor Labs solo revela información confidencial o privada si es requerida judicialmente o por autoridad competente en el marco de procedimientos administrativos.

En virtud de la Ley de Protección de Datos Personales N° 25.326 y del artículo 21, inciso h) de la Ley N° 25.506, el solicitante o titular de un certificado puede solicitar el acceso a toda la información relativa a sus tramitaciones.

Egregor Labs garantiza el acceso permanente, irrestricto y gratuito a la información publicada en su repositorio.

3. Identificación y autenticación

En esta sección se describen los procedimientos empleados por Egregor Labs y su Autoridad de Registro para autenticar la identidad de los solicitantes de certificados como requisito previo a su emisión, y los pasos para autenticar a los solicitantes de renovación y revocación.

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 y de los datos del RENAPER, de acuerdo con el apartado siguiente. Los nombres son nombres distintivos X.500 (Distinguished Names), conforme al Anexo IV de la Resolución SICYT N° 11/2025.

3.1.2. Necesidad de nombres distintivos

Certificados de personas humanas:

- "commonName" (OID 2.5.4.3, nombre común): presente; corresponde al nombre y apellido que figuran en el DNI del suscriptor, según los datos devueltos por el RENAPER.
- "serialNumber" (OID 2.5.4.5, número de serie): presente; contiene el tipo y número de identificación del titular, expresado como texto con el formato "[tipo de documento] [número]". El tipo es "CUIL" o "CUIT", según corresponda.
- "countryName" (OID 2.5.4.6, código de país): presente; representa el país de emisión del certificado, codificado según ISO 3166 de dos (2) caracteres ("AR").

Certificados de personas jurídicas públicas o privadas:

- "commonName" (OID 2.5.4.3, nombre común): coincide con la denominación de la persona jurídica o con el nombre de la unidad operativa responsable (por ejemplo, "Gerencia de Compras").
- "organizationalUnitName" (OID 2.5.4.11, nombre de la suborganización): optativo; contiene las unidades operativas relacionadas con el suscriptor y puede tener varias instancias.
- "organizationName" (OID 2.5.4.10, nombre de la organización): presente; coincide con la denominación de la persona jurídica según su instrumento constitutivo inscripto.
- "serialNumber" (OID 2.5.4.5, número de serie): presente; contiene el número de identificación de la persona jurídica, con el formato "[código de identificación] [número]". Los valores posibles del código son "CUIT", para personas jurídicas argentinas, e "ID [país]", para personas jurídicas extranjeras con número de identificación tributaria de su país, codificado el país según ISO 3166 de dos (2) caracteres.
- "countryName" (OID 2.5.4.6, código de país): presente; "AR".

3.1.3. Anonimato o uso de seudónimos

No se emiten certificados anónimos ni cuyo nombre distintivo contenga un seudónimo.

3.1.4. Reglas para la interpretación de nombres

Todos los nombres representados en los certificados coinciden con los del documento de identidad del suscriptor, según los registros del RENAPER, o con la documentación presentada por la persona jurídica. Se codifican en UTF-8. Las discrepancias que puedan generarse por caracteres especiales se tratan de modo de asegurar la precisión de la información contenida en el certificado, sin alterar el nombre.

3.1.5. Unicidad de nombres

El nombre distintivo es único para cada suscriptor. Puede existir más de un certificado con igual nombre distintivo si corresponde al mismo suscriptor; en particular, un suscriptor puede tener un certificado vigente por cada dispositivo compatible en el que haya generado un par de claves, cada uno con su propio par de claves. Las homonimias se resuelven por el número de CUIL o CUIT incluido en el “serialNumber”.

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, excepto en certificados de personas jurídicas, en los que se acepta la denominación que surja de la documentación presentada. Egregor Labs se reserva el derecho de tomar las decisiones referidas a posibles conflictos sobre la utilización y titularidad de cualquier nombre entre sus suscriptores. En caso de conflicto, la parte que solicite el certificado debe demostrar su interés legítimo y su derecho a utilizar el nombre.

3.2. Registro inicial

Se describen los procedimientos para autenticar, como paso previo a la emisión de un certificado, la identidad y demás atributos del solicitante ante la AR CENTRAL. Las solicitudes se reciben únicamente a través de la aplicación habilitada AdES; en la modalidad presencial, el solicitante la usa en su propio dispositivo ante el Oficial de Registro. La aceptación de la solicitud y la emisión del certificado se comunican en la aplicación habilitada y por correo electrónico.

Egregor Labs cumple con lo establecido en:

a) El artículo 21, inciso a) de la Ley N° 25.506, el artículo 21, inciso 7 del Anexo al Decreto N° 182/2019 y el artículo 15 del Anexo I de la Resolución SICYT N° 11/2025, relativos a la información a brindar a los solicitantes.
b) El artículo 14, inciso b) de la Ley N° 25.506, relativo a los contenidos mínimos de los certificados.
c) El artículo 16 del Anexo I de la Resolución SICYT N° 11/2025, relativo al consentimiento del solicitante para la emisión de certificados.

3.2.1. Métodos para comprobar la titularidad del par de claves

Egregor Labs comprueba que el solicitante es titular del par de claves mediante la verificación de la solicitud de certificado en formato PKCS#10, que no incluye la clave privada. Las claves siempre son generadas por el solicitante. En ningún caso Egregor Labs ni su Autoridad de

Registro pueden tomar conocimiento, exigir o acceder a la clave privada de los solicitantes o titulares, conforme al artículo 21, inciso b) de la Ley N° 25.506 y al artículo 21, inciso 3 del Anexo al Decreto N° 182/2019.

El procedimiento es el siguiente:

- El solicitante genera su par de claves desde la aplicación habilitada, en el módulo criptográfico de su dispositivo. La clave se crea como no exportable, accesible solo en ese dispositivo, solo con el código de desbloqueo configurado, y solo con la biometría registrada al momento de su creación junto con la contraseña de firma que el solicitante define en ese momento. La clave privada no sale del módulo y no queda almacenada en ningún sistema de Egregor Labs.
- La aplicación habilitada arma la CSR con la clave pública y los datos del solicitante, y la firma con la clave privada nueva, lo que requiere la autenticación biométrica del solicitante y su contraseña de firma.
- La aplicación habilitada obtiene de la AR un desafío de un solo uso y genera una atestación de la aplicación cuyo dato firmado incluye el resumen criptográfico (SHA-256) del desafío y de la CSR.
- La AR verifica la firma de la CSR con la clave pública contenida en ella, lo que demuestra la posesión de la clave privada, y verifica la atestación de la aplicación: la cadena de certificados hasta la raíz de App Attest de Apple, el identificador de la aplicación habilitada, el desafío y el contador de uso.
- Si alguna verificación falla, la solicitud se rechaza.

3.2.2. Autenticación de la identidad de personas jurídicas públicas o privadas

Los procedimientos de autenticación de los solicitantes responsables de certificados de personas jurídicas públicas o privadas cumplen los siguientes aspectos:

a) La AR CENTRAL verifica la documentación pertinente relacionada con la solicitud. Este proceso incluye la validación de la identidad del solicitante y la verificación de su condición de representante de la persona jurídica.
b) El requerimiento se efectúa únicamente por intermedio del responsable autorizado por la persona jurídica.
c) La identificación de la persona jurídica titular del certificado se verifica mediante documentación que acredite su condición de tal.

Egregor Labs cumple con las exigencias impuestas por el artículo 21, inciso i) de la Ley N° 25.506, relativo a la conservación de la documentación de respaldo de los certificados emitidos; por el inciso f) del mismo artículo, relativo a la recolección de datos personales; y por el artículo 21, inciso 14 del Anexo al Decreto N° 182/2019, relativo a la protección de datos personales.

El representante legal o apoderado presenta, a través de la aplicación habilitada o ante la AR CENTRAL, la siguiente documentación, como documento electrónico firmado digitalmente o como copia certificada por escribano público:

a) Estatuto o contrato social de la persona jurídica, o norma de creación en el caso de personas jurídicas públicas.

b) Constancia de inscripción en el registro público correspondiente.
c) Constancia de inscripción ante la ARCA (CUIT).
d) Acta de designación de autoridades y de distribución de cargos vigente, o documento que acredite la representación invocada.
e) Poder general amplio o poder especial que autorice a solicitar certificados de firma digital, cuando el solicitante sea apoderado. El modelo de poder especial se publica en el sitio web.
f) DNI de todos los socios, en el caso de sociedades no constituidas regularmente.

El Oficial de Registro verifica la vigencia de la persona jurídica, la suficiencia del cargo o del poder y la coincidencia entre el representante y la persona cuya identidad fue validada, y puede consultar los registros públicos y requerir documentación adicional. La identidad del representante se valida conforme al punto 3.2.3, en cualquiera de sus modalidades.

Se conserva la documentación que respalda el proceso de identificación de la persona responsable de la custodia de las claves criptográficas. El responsable autorizado presta su consentimiento expreso, firmando en la aplicación habilitada con la clave nueva, de que la información incluida en el certificado es correcta.

3.2.3. Autenticación de la identidad de personas humanas

Conforme al artículo 2° del Decreto N° 743/2024, la presencia física del solicitante, suscriptor o representante legal ante la Autoridad de Registro es optativa. En todos los casos, la identidad se verifica con el servicio de validación de identidad del RENAPER, como requisito previo a la emisión, la renovación y la revocación del certificado, con las excepciones de revocación previstas en el punto 3.4.

Egregor Labs cumple con las exigencias impuestas por:

a) El artículo 21, inciso i) de la Ley N° 25.506, relativo a la conservación de la documentación de respaldo de los certificados emitidos.
b) El artículo 21, inciso f) de la Ley N° 25.506, relativo a la recolección de datos personales.
c) El artículo 21, inciso 3 del Anexo al Decreto N° 182/2019, relativo a no generar, exigir ni tomar conocimiento de la clave privada del suscriptor.
d) El artículo 21, inciso 14 del Anexo al Decreto N° 182/2019, relativo a la protección de datos personales.
e) Las Pautas Técnicas y Procedimientos para la Toma de Datos Biométricos del Anexo III de la Resolución SICYT N° 11/2025.

Adicionalmente, Egregor Labs celebra con el solicitante un acuerdo conforme al Anexo V de la Resolución SICYT N° 11/2025, del que surge su conformidad respecto de la veracidad de la información incluida en el certificado.

La AR verifica que el dispositivo del solicitante cumpla las especificaciones del punto 6.2.11.

a) Modalidad remota (presencia telemática).

1. El solicitante ingresa en la aplicación habilitada su CUIL o CUIT y su sexo según el DNI.

2. La aplicación habilitada captura la fotografía digital del rostro con prueba de vida, siguiendo las recomendaciones del Anexo III de la Resolución SICYT N° 11/2025: rostro completamente visible, de frente y alineado, sin inclinación; expresión neutra con la boca cerrada; ojos abiertos, visibles y mirando a la cámara, sin anteojos oscuros ni cabello que los cubra; fondo uniforme y claro, sin sombras ni objetos; iluminación uniforme y sin reflejos; resolución suficiente para el reconocimiento facial; y rostro ocupando aproximadamente el 70 al 80 % de la imagen. La aplicación guía al solicitante para cumplir estas condiciones antes de la captura y no permite cargar imágenes desde la galería del dispositivo.
3. La aplicación envía la captura cifrada a la AR CENTRAL, que la remite al RENAPER para su cotejo en tiempo real.
4. Si el cotejo es negativo, se admiten dos (2) reintentos. Si después del segundo reintento el cotejo sigue siendo negativo, la solicitud no continúa por esta vía y el solicitante puede optar por la modalidad presencial.
5. Si el cotejo es positivo, la AR obtiene del RENAPER los datos de identificación del solicitante, que son los únicos que se incluyen en el certificado.

b) Modalidad presencial.

El solicitante concurre a la AR CENTRAL con su DNI y su dispositivo compatible. El Oficial de Registro, que previamente conecta su token y se autentica con su certificado de firma digital en el sistema del RENAPER:

1. Controla el DNI e ingresa el sexo y el CUIL del solicitante.
2. Captura la fotografía digital del rostro, con las recomendaciones indicadas en el inciso a), y la envía al RENAPER para su verificación.
3. Captura al menos dos (2) huellas dactilares distintas, comenzando por el pulgar izquierdo y el pulgar derecho; si la persona no cuenta con alguno de esos dedos, selecciona otro; si posee un solo dedo, captura la misma huella dos veces; y si existe imposibilidad física para la captura, lo indica con la opción correspondiente e ingresa el motivo. Las capturas cumplen una resolución de al menos 500 ppi, con contraste adecuado, en formato WSQ o ISO/IEC 19794-2.
4. Envía las huellas al RENAPER para su cotejo. Ante un error en la captura de cualquiera de los datos biométricos, realiza dos (2) reintentos.

Solo se procede a la emisión, renovación o revocación si se cumple alguna de estas condiciones: (1) el control biométrico de la huella o del rostro es positivo; (2) el control de la huella, luego del segundo reintento, es negativo y el del rostro es positivo; (3) el control de la huella no puede realizarse por un impedimento físico y el del rostro es positivo, con indicación del motivo; o (4) el control del rostro, luego del segundo reintento, es negativo y el de la huella es positivo. En cualquier otro caso, el Oficial de Registro se abstiene de continuar el trámite.

A requerimiento del solicitante, cuando por motivos religiosos o de tratamientos de salud se requiera la cobertura del cabello, la fotografía puede tomarse con el cabello cubierto siempre que sean visibles los rasgos principales del rostro; y cuando por motivos religiosos el rostro esté cubierto parcial o totalmente, el trámite y la fotografía se realizan en un recinto reservado y por agentes del mismo sexo.

Con la identidad validada, el solicitante completa en su dispositivo la generación de claves y la CSR conforme al punto 3.2.1, y acepta el Acuerdo con Suscriptores. El Oficial de Registro aprueba la solicitud con su certificado de firma digital.

En ambas modalidades se conserva una copia digital de la documentación de respaldo del proceso de autenticación: el resultado del cotejo del RENAPER, la captura del rostro y, en su caso, de las huellas, los reintentos, la CSR, la atestación de la aplicación y la aceptación del Acuerdo con Suscriptores.

3.2.4. Protocolo de contingencia ante fallos en el sistema de biometría para la validación de identidad

Ante dos (2) reintentos fallidos atribuibles exclusivamente al sistema de biometría del RENAPER, se habilita al solicitante a continuar el trámite en forma presencial ante un Oficial de Registro, que realiza la toma de datos biométricos, documenta las fallas y valida la identidad con el número de trámite (ID) del DNI mediante el Sistema de Identidad Digital (SID) del RENAPER.

La AR CENTRAL conserva, para el legajo del suscriptor, la documentación presentada como respaldo del proceso de identificación y los antecedentes de los reintentos fallidos que dieron inicio al procedimiento de contingencia.

3.2.5. Información no verificada del suscriptor

Se conserva la información referida al solicitante que no hubiera sido verificada, conforme al apartado 3 del inciso b) del artículo 14 de la Ley N° 25.506. Ningún dato no verificado se incluye en el certificado.

3.2.6. Validación de autoridad

Según lo dispuesto en el punto 3.2.2, la AR CENTRAL verifica la autorización de la persona humana que actúa en nombre de la persona jurídica para gestionar el certificado. Si la representación cesa o el poder se revoca o vence, la persona jurídica o el responsable deben solicitar la revocación del certificado.

3.2.7. Criterios para la interoperabilidad

Los certificados emitidos pueden ser utilizados por sus titulares en forma interoperable para firmar digitalmente cualquier documento o transacción, y para autenticación o cifrado, conforme al punto 1.4.

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

En los certificados de personas humanas o jurídicas, la renovación con nuevo par de claves aplica a la generación de un nuevo par de claves y su correspondiente certificado: (a) después de la revocación de un certificado; (b) después de la expiración de un certificado; o (c) antes de la expiración de un certificado.

En los casos a) y b) se exige el cumplimiento de los procedimientos del punto 3.2.3.

En el caso c), si el certificado está vigente y no fue revocado, no se exige la presencia física del suscriptor: el suscriptor remite desde la aplicación habilitada la constancia de inicio del trámite de renovación firmada digitalmente con el certificado a renovar. La renovación sin presencia física bajo esta modalidad puede realizarse una sola vez, siempre que no se modifique ningún dato del certificado y que el suscriptor conserve el acceso a su clave privada vigente. Sin perjuicio de ello, la AR CENTRAL repite en todos los casos la validación remota de identidad con el RENAPER del punto 3.2.3.a), que no requiere presencia física.

En los certificados de personas jurídicas, el solicitante presenta nuevamente la documentación del punto 3.2.2.

Como el par de claves está ligado al dispositivo, la renovación también aplica cuando el suscriptor cambia de dispositivo o cuando la clave anterior deja de poder usarse por un cambio de los datos biométricos registrados en el dispositivo; en ese caso el certificado anterior se revoca conforme al punto 4.9.

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

No se admite. Toda renovación implica la generación de un nuevo par de claves en el módulo criptográfico del dispositivo, conforme al punto 3.3.1.

3.4. Requerimiento de revocación

La revocación puede ser solicitada por el suscriptor, por la persona jurídica titular, por la AR CENTRAL o por Egregor Labs, y por las demás personas indicadas en el punto 4.9.2. Como revocar un certificado no permite a nadie firmar en nombre del suscriptor, Egregor Labs facilita la revocación: no exige códigos especiales, autenticación biométrica ni la contraseña de firma. El suscriptor escribe la frase “revocar mi certificado” para confirmar que no lo hace por error, y puede indicar el motivo. Puede identificarse por cualquiera de estas vías:

a) **Desde su cuenta**, en la aplicación habilitada AdES (en cualquier dispositivo) o en el portal web https://advancedelectronicsignature.com/cuenta desde cualquier navegador, con la sesión iniciada. Esta vía permite revocar de inmediato tanto el certificado del dispositivo que está usando como el de un dispositivo perdido o robado.
b) **Mediante validación de identidad ante la Mesa de Ayuda**, por videollamada en vivo con un Oficial de Registro, que compara el rostro y el DNI físico que la persona muestra a cámara con la foto y los datos validados con el RENAPER al emitir el certificado, o en forma presencial ante la AR CENTRAL, cuando el suscriptor no puede acceder a su dispositivo ni a su cuenta. La videollamada no se graba; el Oficial registra los controles realizados.

Las vías a), b) y d) permiten la revocación inmediata en cualquier momento, aun sin servicio del RENAPER. La vía d) solo puede dejar sin efecto un certificado, nunca emitirlo ni usarlo, por lo que su riesgo se limita a una revocación no deseada; para mitigarlo, Egregor Labs notifica cada inicio de sesión y cada revocación por correo electrónico y en la aplicación, y registra la dirección IP y el método de inicio de sesión. La vía c) aplica las Pautas Técnicas para la Toma de Datos Biométricos.

La AR CENTRAL o Egregor Labs inician la revocación en los casos del punto 4.9.1, con la documentación que acredite la causa, a través de la aplicación de la AR, con autenticación de doble factor. La acción queda registrada.

Las personas jurídicas titulares de certificados se obligan a: (1) notificar a la AR CENTRAL toda modificación en la situación del responsable que lo inhabilite para custodiar la clave o que modifique la información contenida en el certificado; y (2) solicitar la revocación inmediata del certificado en esos casos.

4. Ciclo del certificado: requerimientos operativos

4.1. Solicitud de certificado

4.1.1. Solicitantes de certificados

Pueden solicitar certificados las personas humanas y las personas jurídicas indicadas en el punto 1.3.3. Las condiciones que deben cumplir son:

- Contar con DNI argentino vigente y con CUIL o CUIT; en el caso de personas jurídicas, con CUIT y con la documentación del punto 3.2.2.
- Contar con un dispositivo compatible según el punto 6.2.11, con código de desbloqueo y autenticación biométrica configurados, y con la aplicación habilitada AdES instalada desde la tienda oficial de aplicaciones en una versión no inferior a la mínima publicada.
- Contar con una dirección de correo electrónico propia, que se verifica durante la solicitud.
- Contar con un plan asignado según el punto 9.1 (prueba gratuita, plan pago, convenio o exención).

4.1.2. Solicitud de certificado

En el caso de personas humanas, la solicitud solo puede ser iniciada por el propio solicitante. En el caso de personas jurídicas, la solicitud es presentada por el representante legal o por el apoderado con poder suficiente. El solicitante presenta la documentación prevista en los puntos 3.2.2 y 3.2.3 y la constancia de CUIT o CUIL, que la AR verifica.

a) Solicitud de certificado de persona humana. El solicitante:

1. Instala la aplicación habilitada AdES, crea su cuenta y verifica su dirección de correo electrónico con un código de un solo uso.
2. Elige la opción de solicitar un certificado de firma digital. La aplicación verifica que el dispositivo y la versión del sistema operativo sean compatibles según el punto 6.2.11; si no lo son, informa el motivo y no permite continuar.
3. Toma conocimiento de esta Política, del Acuerdo con Suscriptores, de los Términos y Condiciones con Terceros Usuarios y de la Política de Privacidad, que la aplicación presenta antes de continuar, y presta su consentimiento para el cotejo de sus datos con el RENAPER. La aplicación le informa que contrata con Jacobs Comercial S.R.L. (Egregor Labs).

4. Valida su identidad conforme al punto 3.2.3, en la modalidad remota o presencial.
5. Revisa los datos que contendrá el certificado, obtenidos del RENAPER, y presta su conformidad respecto de su veracidad.
6. Genera el par de claves en el módulo criptográfico del dispositivo y la aplicación arma y firma la CSR, que envía a la AR junto con la atestación de la aplicación, conforme al punto 3.2.1.
7. Lee y acepta el Acuerdo con Suscriptores. Al recibir el certificado, lo firma digitalmente con él, lo que constituye además la aceptación del certificado (punto 4.4).
8. Elige su plan según el punto 9.1: la prueba gratuita o un plan pago, salvo que Egregor Labs ya le haya asignado un plan por convenio o exención.

b) Solicitud de certificado de persona jurídica. El representante legal o apoderado:

1. Cumple los pasos 1 a 3 del inciso a).
2. Elige la opción de certificado de persona jurídica e ingresa la denominación y el CUIT de la persona jurídica y, si corresponde, la unidad operativa que integrará el certificado.
3. Adjunta la documentación del punto 3.2.2, o indica que la presentará en forma presencial ante la AR CENTRAL.
4. Valida su propia identidad conforme al punto 3.2.3.
5. Una vez aprobada la documentación por un Oficial de Registro, revisa los datos que contendrá el certificado y presta su conformidad.
6. Cumple los pasos 6 a 8 del inciso a).

Cada solicitud genera un par de claves en un único dispositivo. Para usar la firma digital en otro dispositivo, el suscriptor tramita un certificado adicional desde ese dispositivo, con su propio par de claves y su propia validación de identidad.

4.2. Procesamiento de la solicitud del certificado

La AR CENTRAL acepta la solicitud solo si se cumplen todas estas condiciones:

a) Validación positiva de la identidad del solicitante con el RENAPER, conforme al punto 3.2.3, o el procedimiento de contingencia del punto 3.2.4.
b) Coincidencia entre los datos de la CSR y los datos validados.
c) Firma válida de la CSR con la clave pública que contiene, y clave pública no utilizada en ningún certificado anterior.
d) Atestación de la aplicación válida para esa solicitud, conforme al punto 3.2.1.
e) Dispositivo y versión de sistema operativo admitidos según el punto 6.2.11.
f) En el caso de personas jurídicas, documentación aprobada por un Oficial de Registro según el punto 3.2.2.
g) Aceptación del Acuerdo con Suscriptores y plan asignado según el punto 9.1.

En la modalidad remota, si se cumplen todas las condiciones, la aprobación es automática y se registra con la identificación del sistema de la AR. Si alguna verificación presenta una observación que no implica rechazo (por ejemplo, una diferencia de formato en el nombre), la solicitud se deriva a un Oficial de Registro, que la resuelve dentro de los dos (2) días hábiles. En

la modalidad presencial y en todas las solicitudes de personas jurídicas, el Oficial de Registro aprueba la solicitud firmándola con su certificado en la aplicación de la AR.

Si la solicitud es rechazada, se informa al solicitante el motivo en la aplicación habilitada y por correo electrónico, salvo que hacerlo comprometa la seguridad del proceso. Las solicitudes no completadas dentro de los treinta (30) días corridos se dan de baja.

La AR CENTRAL arma el legajo del suscriptor, que contiene la solicitud, la CSR, la atestación de la aplicación, el resultado del cotejo del RENAPER y los reintentos, en su caso los antecedentes de la contingencia, la documentación de la persona jurídica y el Acuerdo con Suscriptores aceptado.

El solicitante puede consultar en la aplicación habilitada el estado de su trámite y solicitar toda la información relativa a él, conforme al artículo 21, inciso h) de la Ley N° 25.506 y al artículo 21, inciso 7 del Anexo al Decreto N° 182/2019.

4.3. Emisión del certificado

4.3.1. Proceso de emisión del certificado

Cumplidos los recaudos del proceso de identificación y autenticación de esta Política y aprobada la solicitud por la AR CENTRAL, la Autoridad Certificante de Egregor Labs emite el certificado y lo firma digitalmente con su clave privada, alojada en un módulo de seguridad de hardware (HSM), conforme al perfil del punto 7.1. El mismo procedimiento se aplica a la emisión de un certificado por renovación.

La AR entrega el certificado a la aplicación habilitada en el dispositivo en el que se generó el par de claves. La aplicación verifica que la clave pública del certificado corresponda a la clave privada del módulo y lo instala.

4.3.2. Notificación de emisión

La emisión se notifica al suscriptor en la aplicación habilitada y por correo electrónico a la dirección verificada. En la aplicación, cada suscriptor accede únicamente a su propia información.

4.4. Aceptación del certificado

Antes de la emisión, el suscriptor presta conformidad con los datos que contendrá el certificado, conforme al punto 4.1.2. Una vez emitido, la aplicación habilitada le muestra el contenido del certificado y le solicita que lo acepte firmando digitalmente con él el Acuerdo con Suscriptores, en un solo paso con su biometría y su contraseña de firma. Esa firma constituye la aceptación expresa del certificado, y el Acuerdo firmado se conserva en el legajo. El certificado no puede usarse para firmar otros documentos hasta que el Acuerdo esté firmado.

Si existiera algún error u omisión en los datos, el suscriptor debe rechazarlo desde la aplicación, lo que provoca su revocación inmediata, o solicitar su revocación por las vías del punto 3.4 dentro de las cuarenta y ocho (48) horas de la notificación. Ante la ausencia de reclamos dentro de ese plazo, o con la primera firma realizada con el certificado, se considera aceptada la

exactitud de su contenido y el suscriptor asume las obligaciones y responsabilidades de esta Política.

No se notifica la emisión a otras entidades. Los certificados emitidos pueden consultarse en el repositorio según el punto 2.2.

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 el artículo 25 de la Ley N° 25.506, el suscriptor debe:

a) Mantener el control exclusivo de sus datos de creación de firma digital, no compartirlos e impedir su divulgación. En particular, no debe registrar en su dispositivo la biometría de otra persona ni compartir el código de desbloqueo.
b) Utilizar un dispositivo de creación de firma digital técnicamente confiable: un dispositivo compatible según el punto 6.2.11, sin modificaciones que alteren sus controles de seguridad (por ejemplo, con el sistema operativo liberado o "jailbreak") y con la aplicación habilitada AdES obtenida de la tienda oficial.
c) Solicitar la revocación de su certificado ante cualquier circunstancia que pueda haber comprometido la privacidad de sus datos de creación de firma, incluida la pérdida, el robo o la entrega a terceros del dispositivo.
d) Informar sin demora al Certificador el cambio de alguno de los datos contenidos en el certificado que hubiera sido objeto de verificación.

Asimismo, el suscriptor debe:

a) Resguardar y no divulgar los factores de autenticación que permiten utilizar la clave privada o gestionar el certificado: la contraseña de firma, el código de desbloqueo del dispositivo, y la contraseña de su cuenta en la aplicación.
b) Proveer de modo completo y preciso toda la información que le sea requerida para la emisión del certificado.
c) Utilizar los certificados de acuerdo con esta Política.
d) Tomar debido conocimiento del contenido de esta Política, del Manual de Procedimientos, del Acuerdo con Suscriptores y de cualquier otro documento aplicable, que la aplicación habilitada presenta antes de la solicitud y que se publican en el repositorio.

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 esta Política.
b) Verificar la validez del certificado digital: su firma, su cadena de certificación hasta la AC-RAÍZ, su período de validez y su estado de revocación al momento de la firma, mediante la CRL o el servicio OCSP.

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

Se aplica el punto 3.3.2: no se admite.

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

Se aplican los procedimientos del punto 3.3.1. La aplicación habilitada avisa al suscriptor treinta (30) días antes del vencimiento de su certificado. El nuevo certificado tiene un nuevo período de validez. Si el certificado anterior estaba vigente, se revoca al aceptarse el nuevo cuando ambos estén asociados al mismo dispositivo.

4.8. Modificación del certificado

El suscriptor está obligado a notificar a Egregor Labs cualquier cambio en los datos contenidos en el certificado que hubieran sido objeto de verificación, conforme al inciso d) del artículo 25 de la Ley N° 25.506. En tal caso, procede la revocación del certificado y, de ser requerido, la solicitud de uno nuevo.

4.9. Suspensión y revocación de certificados

Los certificados se revocan en los plazos del punto 4.9.5, sobre la base de una solicitud de revocación validada según el punto 4.9.3. El estado de suspensión no está contemplado en la legislación vigente aplicable a la firma digital.

4.9.1. Causas de revocación

Egregor Labs revoca los certificados que hubiera emitido en los siguientes casos:

a) A solicitud del titular del certificado o del responsable autorizado, en el caso de certificados de personas jurídicas.
b) Si 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 o de 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, incluido el cese de la representación o la revocación o el vencimiento del poder del responsable de un certificado de persona jurídica, o la disolución de la persona jurídica.
j) Cuando la clave privada asociada al certificado, o el medio en que se encuentra almacenada, están comprometidos o corren peligro de estarlo. Comprende, entre otros casos: la pérdida o el robo del dispositivo; su entrega a un tercero sin borrado previo; la modificación de los datos biométricos registrados en el dispositivo; y la detección de que

el módulo criptográfico de un modelo o versión de sistema operativo admitido presenta una vulnerabilidad que permite extraer o usar la clave sin la autenticación del titular.

k) Ante el 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 con esta Política, el Manual de Procedimientos, la Ley N° 25.506, su modificatoria y sus normas reglamentarias.
m) Por revocación del certificado de la AC EGREGOR.
n) Cuando el suscriptor elimina su cuenta en la aplicación habilitada, en cuyo caso se revocan todos los certificados asociados a ella.

4.9.2. Autorizados a solicitar la revocación

Están autorizados a solicitar la revocación de un certificado:

a) En el caso de certificados de personas humanas, el suscriptor.
b) En el caso de certificados de personas jurídicas, el responsable autorizado que efectuó el requerimiento.
c) En el caso de certificados de personas jurídicas, el responsable debidamente autorizado por la persona jurídica titular del certificado.
d) Egregor Labs o la AR CENTRAL.
e) El Ente Licenciante.
f) La autoridad judicial.
g) La Autoridad de Aplicación.

4.9.3. Procedimientos para la solicitud de revocación

Las vías disponibles para solicitar la revocación son:

Vía	Dirección	Quién la usa
Cuenta, en la aplicación habilitada AdES o en el portal web	Opción “Revocar” en Perfil, o https://advancedelectronicsignature.com/cuenta, con la frase “revocar mi certificado”	Suscriptor con sesión iniciada, desde cualquier dispositivo o navegador
Mesa de Ayuda, con validación de identidad por videollamada en vivo, o AR CENTRAL en forma presencial	Teléfono [●] o ayuda@advancedelectronicsignature.com para coordinar la videollamada, las 24 horas, o en forma presencial	Suscriptor sin acceso a su dispositivo ni a su cuenta
Nota firmada digitalmente u ológrafa con firma certificada	ar@advancedelectronicsignature.com o domicilio de la AR CENTRAL	Persona jurídica titular, Ente Licenciante, autoridad judicial, Autoridad de Aplicación
Aplicación de la AR	Acceso interno con doble factor	Egregor Labs y AR CENTRAL

Egregor Labs garantiza que:

a) Se identifica debidamente al solicitante de la revocación según el punto 3.4.
b) Las solicitudes de revocación y toda acción efectuada por el Certificador o la AR en el proceso están documentadas y conservadas en sus archivos.
c) Se documentan y archivan las causales de las revocaciones aprobadas.
d) Una vez efectuada la revocación, se actualiza el estado del certificado en el repositorio y en el servicio OCSP y se lo incluye en la próxima Lista de Certificados Revocados.
e) El suscriptor del certificado revocado es informado del cambio de estado en la aplicación habilitada y por correo electrónico. En el caso de certificados de personas jurídicas, también se informa a la persona jurídica titular.

4.9.4. Plazo para la solicitud de revocación

Ante cualquiera de las circunstancias del punto 4.9.1, la revocación debe solicitarse en forma inmediata. El servicio de recepción de solicitudes de revocación está disponible en forma permanente, siete (7) días por veinticuatro (24) horas, conforme al artículo 21, inciso 8 del Anexo al Decreto N° 182/2019.

4.9.5. Plazo para el procesamiento de la solicitud de revocación

Egregor Labs revoca el certificado en un plazo no superior a las veinticuatro (24) horas de recibido el requerimiento. Las solicitudes efectuadas desde la cuenta, en la aplicación habilitada o en el portal web, se procesan en forma automática e inmediata.

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 como mínimo equivalentes, como el servicio OCSP del punto 4.9.10.

La autenticidad y validez de las Listas de Certificados Revocados se confirma mediante la verificación de la firma digital de la AC EGREGOR y de su período de validez.

Egregor Labs cumple con lo establecido en el artículo 21, inciso 9 del Anexo al Decreto N° 182/2019, relativo al acceso al repositorio de certificados revocados, y con las obligaciones de la Resolución SICYT N° 11/2025.

4.9.7. Frecuencia de emisión de listas de certificados revocados

Egregor Labs genera y publica una única lista que contiene, en forma acumulativa, todos los certificados revocados por ella, en formato CRL X.509 versión 2. Emite una nueva lista dentro de la hora de cada revocación y, en todo caso, cada doce (12) horas, sin superar nunca las veinticuatro (24) horas entre publicaciones.

4.9.8. Vigencia de la Lista de Certificados Revocados

Cada lista tiene una vigencia de veinticuatro (24) horas e indica en el campo “nextUpdate” la fecha de emisión de la siguiente.

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

Egregor Labs pone a disposición de los interesados la verificación del estado de un certificado mediante la Lista de Certificados Revocados y mediante el servicio OCSP. Egregor Labs presta ambos servicios en forma obligatoria; los terceros usuarios pueden usar cualquiera de ellos.

a) Lista de Certificados Revocados: https://advancedelectronicsignature.com/crl/ac-egregor.crl, replicada en https://[dominio alternativo]/crl/ac-egregor.crl.
b) Servicio OCSP: https://ocsp.advancedelectronicsignature.com.
c) Ambos servicios están disponibles siete (7) días por veinticuatro (24) horas.

Si alguno de los servicios no está disponible, los terceros usuarios pueden usar el otro. Egregor Labs restablece el servicio conforme a los plazos del Plan de Contingencia e informa la interrupción en su sitio web.

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

El servicio OCSP responde conforme al RFC 6960 y al perfil del punto 7.3. La respuesta está firmada por el certificado de respondedor OCSP emitido por la AC EGREGOR. Para usarlo, el tercero usuario necesita una aplicación compatible con el protocolo OCSP y conexión a Internet.

4.9.11. Otras formas disponibles para la divulgación de la revocación

Egregor Labs permite buscar un certificado por su número de serie o por el CUIL o CUIT de su titular y consultar su estado en ese instante en https://advancedelectronicsignature.com/consulta. Para usar este servicio basta un navegador web con conexión a Internet.

4.9.12. Requisitos específicos para casos de compromiso de claves

En caso de compromiso de su clave privada, el titular del certificado está obligado a comunicarlo inmediatamente a Egregor Labs mediante alguna de las vías del punto 4.9.3. Si el dispositivo se perdió o fue robado, debe revocar el certificado desde su cuenta, en cualquier dispositivo o navegador, o mediante la validación de identidad con el RENAPER.

4.9.13. Causas de suspensión

El estado de suspensión no está contemplado en el marco de la Ley N° 25.506 y su modificatoria.

4.9.14. Autorizados a solicitar la suspensión

El estado de suspensión no está contemplado en el marco de la Ley N° 25.506 y su modificatoria.

4.9.15. Procedimientos para la solicitud de suspensión

El estado de suspensión no está contemplado en el marco de la Ley N° 25.506 y su modificatoria.

4.9.16. Límites del período de suspensión de un certificado

El estado de suspensión no está contemplado en el marco de la Ley N° 25.506 y su modificatoria.

4.10. Estado del certificado

4.10.1. Características técnicas

Los servicios disponibles para la verificación del estado de los certificados emitidos por Egregor Labs son la Lista de Certificados Revocados (CRL X.509 v2, conforme al punto 7.2) y el servicio OCSP (RFC 6960, conforme al punto 7.3). La CRL se emite según el punto 4.9.7 con una vigencia de veinticuatro (24) horas. El servicio OCSP informa si el certificado está vigente (“good”), revocado (“revoked”) o es desconocido (“unknown”).

4.10.2. Disponibilidad del servicio

Los servicios de distribución de la CRL y de consulta en línea del estado de los certificados están disponibles con un objetivo del noventa y nueve coma nueve por ciento (99,9 %) mensual y un tiempo programado de inactividad máximo del cero coma cinco por ciento (0,5 %) anual. Las tareas de mantenimiento programado nunca impiden la consulta de una CRL vigente.

4.10.3. Aspectos operativos

Los servicios de estado se prestan desde el sitio principal y desde el sitio de contingencia, ambos en la República Argentina. La CRL se replica además en una red de distribución de contenidos.

4.11. Desvinculación del suscriptor

En caso de expiración o revocación del certificado, su titular se considera desvinculado de los servicios de Egregor Labs, excepto que tramite un nuevo certificado. De igual forma se produce la desvinculación ante el cese de las operaciones del Certificador. La desvinculación no afecta la conservación de la documentación según el punto 5.5.

4.12. Recuperación y custodia de claves privadas

En virtud del artículo 21, inciso b) de la Ley N° 25.506 y del artículo 21, inciso 3 del Anexo al Decreto N° 182/2019, Egregor Labs no realiza bajo ninguna circunstancia la recuperación o custodia de claves privadas de los titulares de certificados. El módulo criptográfico del dispositivo no permite la exportación de la clave privada, por lo que ante su pérdida corresponde la revocación del certificado y la emisión de uno nuevo.

Asimismo, el suscriptor está obligado a mantener el control exclusivo de su clave privada, no compartirla e impedir su divulgación, de acuerdo con el artículo 25, inciso a) de la Ley N° 25.506.

5. Controles de seguridad física, operativos y de gestión

Se describen a continuación los controles de seguridad física, de gestión y operativos implementados por Egregor Labs. La descripción detallada se encuentra en el Plan de Seguridad.

5.1. Controles de seguridad física

Egregor Labs cuenta con controles de seguridad relativos a:

a) **Construcción y ubicación de instalaciones.** La infraestructura de la AC, de la AR y de los servicios de estado se aloja en un centro de datos situado en la República Argentina ([●]), en un recinto exclusivo de Jacobs Comercial S.R.L. sin identificación exterior, y el sitio de contingencia en [●], también en el país.
b) **Niveles de acceso físico.** Se aplican los seis (6) niveles de la Sección 4 del Anexo II de la Resolución SICYT N° 11/2025: nivel 1, acceso al edificio con identificación y registro; nivel 2, área interna con registro electrónico; nivel 3, recinto exclusivo con doble método de identificación, donde operan la AR, el repositorio y el OCSP; nivel 4, rack cerrado con los HSM, accesible solo con la presencia simultánea de dos personas autorizadas; niveles 5 y 6, caja de seguridad y compartimento exclusivo para los elementos de activación de la clave de la AC.
c) **Comunicaciones, energía y ambientación.** Alimentación con UPS y grupo electrógeno, climatización redundante y vínculos de comunicaciones de dos proveedores.
d) **Exposición al agua.** Detección de humedad y ubicación de los equipos sobre piso técnico, fuera de zonas inundables.
e) **Prevención y protección contra incendios.** Detección temprana y extinción por agente limpio.
f) **Medios de almacenamiento.** Los medios con copias de respaldo se guardan cifrados en el nivel que corresponde a su clasificación.
g) **Disposición de material de descarte.** Borrado seguro o destrucción física de medios, con registro.
h) **Instalaciones de seguridad externas.** Vigilancia permanente y circuito cerrado de televisión en el centro de datos.

5.2. Controles de gestión

Egregor Labs cuenta con controles de seguridad relativos a:

a) **Definición de roles afectados al proceso de certificación:** Responsable de la AC, Responsable de Seguridad, Operadores de HSM, Custodios de los datos de activación, Administrador de sistemas, Auditor interno, Responsable de la AR, Oficiales de Registro y Responsable de Soporte Técnico.
b) **Número de personas requeridas por función:** toda operación con la clave de la AC requiere la presencia de al menos tres (3) personas autorizadas (control M de N del punto 6.2.2) y la de un testigo del rol de Auditor interno o de Responsable de Seguridad.
c) **Identificación y autenticación para cada rol:** cuentas nominativas con autenticación de doble factor; los Oficiales de Registro se autentican con su certificado de firma digital en un token criptográfico.
d) **Separación de funciones:** una misma persona no puede ser a la vez Operador de HSM y Auditor interno, ni Administrador de sistemas y Custodio de datos de activación. La

aprobación automática de solicitudes remotas por el sistema de la AR no habilita a ningún rol a emitir certificados fuera del flujo aprobado.

5.3. Controles de seguridad del personal

Egregor Labs cuenta con controles de seguridad relativos a:

a) Calificaciones, experiencia e idoneidad del personal, tanto del que cumple funciones críticas como del que cumple funciones administrativas, de seguridad o de limpieza.
b) Antecedentes laborales y certificado de antecedentes penales, verificados antes de asignar un rol de confianza.
c) Entrenamiento y capacitación inicial en esta Política, el Manual de Procedimientos y el Plan de Seguridad.
d) Actualización técnica al menos una vez por año y ante cada cambio relevante de normas o sistemas.
e) Rotación de cargos según las necesidades operativas, preservando la separación de funciones.
f) Sanciones por acciones no autorizadas, según el régimen disciplinario y el acuerdo de confidencialidad.
g) Requisitos para la contratación de personal, que incluyen la firma de un acuerdo de confidencialidad.
h) Documentación provista al personal, incluidas credenciales y otros elementos de identificación, que se devuelven y se dan de baja el mismo día de la desvinculación.

5.4. Procedimientos de auditoría de seguridad

Se mantienen políticas de registro de eventos, cuyos procedimientos detallados se desarrollan en el Manual de Procedimientos. Los procedimientos de auditoría de seguridad comprenden:

a) **Tipos de eventos registrados:** los de la Sección 3 del Anexo II de la Resolución SICYT N° 11/2025, incluidos el ciclo de vida de las claves de la AC, de los certificados y de los dispositivos criptográficos; las solicitudes y su resultado, incluidas las consultas al RENAPER y las verificaciones de la atestación de la aplicación; las revocaciones; y los eventos de seguridad.
b) **Frecuencia de procesamiento de registros:** monitoreo automático continuo con alertas, y revisión semanal por el Responsable de Seguridad.
c) **Período de guarda de los registros:** diez (10) años, conforme al artículo 21, inciso i) de la Ley N° 25.506.
d) **Medidas de protección de los registros:** acceso de solo lectura para los roles de auditoría; los registros se encadenan criptográficamente para detectar cualquier alteración; nunca contienen claves privadas ni contraseñas.
e) **Procedimientos de resguardo de los registros:** copia diaria cifrada al sitio de contingencia.
f) **Sistemas de recolección y análisis de registros:** internos, operados por Egregor Labs.
g) **Notificaciones del sistema de recolección y análisis:** alertas en tiempo real al Responsable de Seguridad ante eventos críticos.

h) **Evaluación de vulnerabilidades:** escaneo mensual de la infraestructura, análisis de seguridad de red al menos cada seis (6) meses y prueba de penetración anual de la infraestructura y de la aplicación habilitada AdES por un tercero independiente.

5.5. Conservación de registros de eventos

Se han desarrollado e implementado políticas de conservación de registros, cuyos procedimientos detallados se encuentran en el Manual de Procedimientos. Los procedimientos cumplen con el artículo 21, inciso i) de la Ley N° 25.506, relativo al mantenimiento de la documentación de respaldo de los certificados emitidos, y con la Sección 3 del Anexo II de la Resolución SICYT N° 11/2025.

Los procedimientos de conservación y guarda comprenden:

a) **Tipo de registro archivado:** registros de eventos de la Sección 3 del Anexo II; legajos de los suscriptores (solicitud, CSR, atestación de la aplicación, resultado del RENAPER, documentación de personas jurídicas, Acuerdo con Suscriptores aceptado); certificados emitidos; solicitudes de revocación y sus causales; CRL emitidas.
b) **Período de guarda:** diez (10) años desde la expiración o revocación del certificado al que se refieren.
c) **Medidas de protección de los registros archivados:** cifrado con claves gestionadas en el HSM y acceso restringido a roles de confianza, con registro de cada acceso.
d) **Procedimientos de resguardo:** copias cifradas en el sitio de contingencia, con prueba de restauración periódica.
e) **Sistemas de recolección y análisis de registros:** internos.
f) **Procedimientos para obtener y verificar la información archivada:** a pedido de autoridad competente o del titular, por el Responsable de Seguridad, con verificación de la integridad del encadenamiento criptográfico.

5.6. Cambio de claves criptográficas

El cambio del par de claves de la AC EGREGOR da origen a la emisión de un nuevo certificado por parte de la AC-RAÍZ. La nueva clave pública se distribuye por los mismos medios que la anterior: se publica en https://advancedelectronicsignature.com/firma-digital y en el sitio de la AC-RAÍZ.

Egregor Labs inicia la renovación de su clave con la anticipación necesaria para que el período de validez restante del certificado de la AC nunca sea inferior al período de validez de los certificados que emite, y en todo caso dos (2) años antes de su vencimiento. Desde ese momento, los nuevos certificados se firman con la clave nueva, y la clave anterior solo se usa para firmar las CRL de los certificados emitidos con ella, hasta su vencimiento.

Si la clave privada de la AC estuviera comprometida, se procede a la revocación de su certificado y esa clave no se usa más para emitir certificados ni CRL.

5.7. Compromiso y recuperación ante desastres

Los requerimientos relativos a la recuperación de los recursos de Egregor Labs en caso de falla o desastre se desarrollan en el Plan de Contingencia, que contiene 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: comunicación inmediata al Ente Licenciante y a la AC-RAÍZ, revocación de todos los certificados emitidos, publicación de una CRL final, notificación a los suscriptores y a los terceros usuarios a través del sitio web, y generación de una nueva clave y certificado de la AC.
d) Continuidad de las operaciones en un entorno seguro luego de desastres, desde el sitio de contingencia.

El Plan de Contingencia contempla además la indisponibilidad de servicios de terceros de los que depende la emisión (el servicio de validación de identidad del RENAPER, el servicio de atestación de Apple y la distribución de la aplicación habilitada AdES), sin que ello afecte la recepción de revocaciones ni los servicios de estado.

Los procedimientos cumplen con el artículo 20 del Anexo al Decreto N° 182/2019, en lo relativo a los servicios de infraestructura tecnológica prestados por terceros.

5.8. Plan de Cese de Actividades

Los requisitos y procedimientos a adoptar en caso de finalización de los servicios de Jacobs Comercial S.R.L. como certificador licenciado se desarrollan en su Plan de Cese de Actividades, que contiene procedimientos referidos a:

a) Notificación al Ente Licenciante, a los suscriptores, a los terceros usuarios, a otros certificadores y a otros usuarios vinculados.
b) Revocación del certificado del Certificador y de los certificados emitidos.
c) Custodia de archivos y documentación e identificación de su custodio, que cumple con idénticas exigencias de seguridad que las previstas para Egregor Labs.

Se contempla la aplicación de la sanción de caducidad de la licencia en los casos del artículo 44 de la Ley N° 25.506 y las causales de cese del artículo 22 de esa ley. Los procedimientos cumplen con el artículo 20 del Anexo al Decreto N° 182/2019 y con las obligaciones de la Resolución SICYT N° 11/2025.

6. Controles de seguridad técnica

Se describen las medidas de seguridad implementadas por Egregor Labs para proteger las claves criptográficas y otros parámetros de seguridad críticos, y los controles técnicos sobre las funciones operativas del Certificador, de la Autoridad de Registro y de los suscriptores.

6.1. Generación e instalación del par de claves criptográficas

Entidad	Responsable de la generación	Método	Clave
AC EGREGOR	Operadores de HSM, con control M de N	Hardware: HSM FIPS 140 nivel 3	ECDSA P-384
Respondedor OCSP	Operadores de HSM	Hardware: HSM FIPS 140 nivel 3	ECDSA P-384
Servicio de aprobación automática de la AR CENTRAL	Operadores de HSM	Hardware: HSM FIPS 140 nivel 3	ECDSA P-384
Oficiales de Registro	Cada Oficial de Registro	Hardware: token FIPS 140 nivel 2 o superior	RSA 2048 o ECDSA P-256 como mínimo
Suscriptores	Cada suscriptor, mediante la aplicación habilitada AdES	Hardware: módulo criptográfico del dispositivo (punto 6.2.11)	ECDSA P-256

6.1.1. Generación del par de claves criptográficas

AC EGREGOR. La clave privada de la AC se genera en un HSM con certificación FIPS 140 nivel 3, en el nivel 4 de seguridad física, durante una ceremonia con la presencia de los custodios requeridos por el control M de N, del Responsable de Seguridad y del Auditor interno, que se documenta en acta y se graba. Se respeta la Sección 2, apartado VI, del Anexo II de la Resolución SICYT N° 11/2025: la clave es única, no puede deducirse, está protegida contra réplicas fraudulentas y contra su uso indebido, y no sale del HSM en forma legible.

Oficiales de Registro. Cada Oficial de Registro genera su clave en su token criptográfico, que no permite exportarla.

Suscriptores. El suscriptor genera su par de claves desde la aplicación habilitada AdES, en el módulo criptográfico de su dispositivo. La clave se genera dentro del módulo con su generador de números aleatorios, nunca existe fuera de él y se crea con los siguientes atributos:

- no exportable;
- accesible solo en ese dispositivo y solo mientras el dispositivo tenga un código de desbloqueo configurado;
- cada uso requiere la autenticación biométrica del titular (Face ID o Touch ID) y, además, la contraseña de firma que el titular define al generar la clave; el módulo exige ambos factores juntos;
- la clave queda inutilizable si se agrega o modifica un dato biométrico registrado en el dispositivo.

La aplicación habilitada no ofrece generación de claves por software ni importación de claves.

6.1.2. Entrega de la clave privada

Egregor Labs cumple con la obligación de abstenerse de generar, exigir o por cualquier otro medio tomar conocimiento o acceder a los datos de creación de firma de los suscriptores y de los Oficiales de Registro, conforme al artículo 21, inciso b) de la Ley N° 25.506 y al artículo 21, inciso 3 del Anexo al Decreto N° 182/2019. No hay entrega de claves privadas: cada titular genera la suya en su propio dispositivo.

6.1.3. Entrega de la clave pública al emisor del certificado

El solicitante entrega su clave pública a Egregor Labs durante la solicitud, dentro de la CSR en formato PKCS#10 firmada con su clave privada ("prueba de posesión"). La aplicación habilitada la envía a la AR CENTRAL por un canal TLS con verificación del certificado del servidor, junto con la atestación de la aplicación, que vincula la CSR con la instancia de la aplicación que la generó, conforme al punto 3.2.1.

6.1.4. Disponibilidad de la clave pública del Certificador

El certificado de la AC EGREGOR, el de la AC-RAÍZ y el del respondedor OCSP están disponibles en un repositorio en línea de acceso público en https://advancedelectronicsignature.com/firma-digital. La aplicación habilitada incluye además los certificados de la cadena para verificar las firmas que produce.

La validez de los certificados de los suscriptores se verifica:

I) Verificando la cadena de confianza: el certificado del suscriptor, firmado por la AC EGREGOR, y el certificado de la AC EGREGOR, firmado por la AC-RAÍZ.
II) Verificando la vigencia y el estado de los certificados mediante las CRL emitidas por la AC EGREGOR y por la AC-RAÍZ, o mediante el servicio OCSP.

6.1.5. Tamaño de claves

Se respetan las longitudes mínimas de la Sección 2, apartado VI.2 del Anexo II de la Resolución SICYT N° 11/2025:

- AC EGREGOR (firma de certificados y CRL): ECDSA de 384 bits (curva P-384).
- Respondedor OCSP: ECDSA de 384 bits (curva P-384).
- Oficiales de Registro: RSA de 2048 bits o ECDSA de 256 bits como mínimo.
- Suscriptores: ECDSA de 256 bits (curva P-256), superior al mínimo de 224 bits.

6.1.6. Generación de parámetros de claves asimétricas

Se usan exclusivamente las curvas elípticas NIST P-256 y P-384 definidas en FIPS 186, con sus parámetros normalizados. No se generan parámetros propios. La AR rechaza toda CSR cuya clave pública no corresponda a la curva P-256 o no sea un punto válido de la curva.

6.1.7. Propósitos de utilización de claves (campo "KeyUsage" en certificados X.509 v3)

Las claves de los suscriptores pueden utilizarse para firmar digitalmente, para funciones de autenticación y para cifrado. Conforme al punto 2.3.3 del Anexo IV de la Resolución SICYT N°

11/2025, la extensión “KeyUsage” de los certificados de personas humanas y jurídicas tiene en UNO (1) los bits “digitalSignature”, “nonRepudiation”, “keyEncipherment” y “dataEncipherment”, y además “keyAgreement”, que corresponde al uso de cifrado de las claves de curva elíptica (punto 1.4). La clave de la AC se usa solo para firmar certificados y CRL (“keyCertSign” y “cRLSign”), y la del respondedor OCSP solo para firmar respuestas OCSP.

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

6.2.1. Controles y estándares para dispositivos criptográficos

- **AC EGREGOR:** HSM con certificación FIPS 140-2 o FIPS 140-3 nivel 3 [marca, modelo y número de certificado CMVP], en el sitio principal y en el de contingencia.
- **Oficiales de Registro:** tokens con certificación FIPS 140-2 o FIPS 140-3 nivel 2 o superior, clasificados como ACTIVOS por el NIST.
- **Suscriptores:** módulo criptográfico del dispositivo, conforme al punto 6.2.11.

6.2.2. Control “M de N” de clave privada

La clave privada de la AC se activa exclusivamente en las instalaciones de Egregor Labs o en su sitio de contingencia, dentro del nivel de seguridad asignado a las operaciones críticas, con la presencia de tres (3) de cinco (5) custodios autorizados. El detalle se desarrolla en el Plan de Seguridad.

Los Oficiales de Registro acceden a su clave con la posesión del token y su contraseña. Los suscriptores acceden a su clave con la posesión del dispositivo, su autenticación biométrica y su contraseña de firma.

6.2.3. Recuperación de clave privada

Egregor Labs puede recuperar la clave privada de su AC a partir de las copias de respaldo del punto 6.2.4, solo con el control M de N, en un HSM de Egregor Labs y en los niveles de seguridad de su sitio principal o de contingencia.

No se implementan mecanismos de respaldo ni de recuperación de las claves privadas de los Oficiales de Registro ni de los suscriptores. Ante su pérdida o compromiso, se revoca el certificado y se tramita uno nuevo.

6.2.4. Copia de seguridad de clave privada

Inmediatamente después de su generación, la clave privada de la AC se copia al HSM del sitio de contingencia y a medios de respaldo cifrados por el propio HSM, mediante los mecanismos del fabricante, sin que la clave exista nunca en forma legible fuera de un HSM. Las copias se custodian en los niveles 5 y 6 de seguridad física, con el mismo control M de N, de modo que su seguridad no disminuye por la existencia de copias.

6.2.5. Archivo de clave privada

Las copias de resguardo de la clave privada de la AC y sus elementos de activación se conservan en lugares seguros, bajo los niveles de seguridad requeridos por la normativa vigente, durante la vida útil de la clave. No se archivan claves privadas de suscriptores ni de Oficiales de Registro.

6.2.6. Transferencia de claves privadas en dispositivos criptográficos

La clave privada de la AC solo se transfiere entre HSM de Egregor Labs, cifrada con los mecanismos del fabricante y con control M de N. Los suscriptores no pueden transferir su clave privada a otro dispositivo: para firmar desde otro dispositivo deben tramitar un nuevo certificado. La clave tampoco se transfiere al restaurar una copia de seguridad del teléfono.

6.2.7. Almacenamiento de claves privadas en dispositivos criptográficos

La clave de la AC se almacena en el HSM y nunca en texto plano fuera de él. Las claves de los Oficiales de Registro se almacenan en sus tokens, que no permiten exportarlas. Las claves de los suscriptores se almacenan en el módulo criptográfico de su dispositivo con los atributos del punto 6.1.1, que no permiten exportarlas.

6.2.8. Método de activación de claves privadas

La clave privada de la AC se activa con el control M de N: los custodios necesarios se identifican ante el HSM, en un orden determinado, con sus credenciales de activación personales. La clave de un Oficial de Registro se activa con la contraseña de su token. La clave de un suscriptor se activa para cada operación de firma con su autenticación biométrica y su contraseña de firma en el dispositivo; la aplicación habilitada AdES muestra antes qué se va a firmar.

6.2.9. Método de desactivación de claves privadas

La clave de la AC se desactiva cerrando la sesión del HSM al finalizar cada ceremonia o, en el servidor de firma en línea, mediante un procedimiento de excepción autorizado por el Responsable de la AC con control M de N. La clave del suscriptor se desactiva automáticamente al terminar cada operación de firma.

6.2.10. Método de destrucción de claves privadas

Al finalizar la vida útil de la clave de la AC, sus copias en el HSM principal, en el de contingencia y en los medios de respaldo se borran e inicializan a cero en una ceremonia con control M de N, que se documenta en acta.

Cuando un certificado de suscriptor se revoca o expira sin renovación, la aplicación habilitada elimina la clave privada y el certificado del dispositivo. La eliminación de la cuenta en la aplicación o de la aplicación misma también elimina la clave.

6.2.11. Requisitos de los dispositivos criptográficos

AC EGREGOR y servicios de la AC: FIPS 140-2 o FIPS 140-3 nivel 3 o superior.

Oficiales de Registro: FIPS 140-2 o FIPS 140-3 nivel 2 o superior, clasificados como ACTIVOS por el NIST.

Suscriptores: conforme a la Sección 2, apartado VI.3.c del Anexo II de la Resolución SICYT N° 11/2025, el módulo criptográfico del dispositivo del suscriptor debe encontrarse clasificado como ACTIVO (ACTIVE) por el NIST. Se admiten dispositivos Apple iPhone con iOS 18 o posterior. El módulo criptográfico de iOS 18 (Apple Secure Enclave Processor / Secure Key Store) cuenta con los certificados CMVP N° 5305 y N° 5306 en estado ACTIVO, vigentes hasta el 2 de junio de 2031.

Apple somete a validación ante el NIST el módulo de cada nueva versión de iOS, y la validación concluye después de su publicación; por ejemplo, el módulo de iOS 26 se encuentra en evaluación ("Implementation Under Test"). Para no impedir la firma digital a quienes actualizan su teléfono, Egregor Labs admite las versiones de iOS posteriores a la mínima cuyo módulo se encuentre en evaluación ante el NIST, y registra para cada certificado la versión de iOS con la que se generó la clave. Si la evaluación de un módulo concluyera sin validación, o el NIST lo clasificara como no válido, Egregor Labs dejará de admitir esa versión, lo notificará a los suscriptores afectados y revocará y sustituirá sin cargo sus certificados conforme al artículo 21, inciso 15 del Anexo al Decreto N° 182/2019. Egregor Labs somete este criterio a la consideración del Ente Licenciante. [Ajustar según lo que resuelva el Ente.]

La aplicación habilitada verifica el modelo y la versión del sistema operativo antes de generar el par de claves y no permite la solicitud en dispositivos o versiones no admitidos. Egregor Labs publica y mantiene actualizado el listado de modelos y versiones admitidos según el punto 2.2.k).

Si un módulo admitido pasa a la clasificación HISTÓRICO (HISTORICAL), se aplica la excepción de la Sección 2, apartado VI.3 del Anexo II: los certificados emitidos pueden seguir utilizándose, pero no más allá de los tres (3) años desde esa reclasificación. Egregor Labs deja de emitir certificados nuevos para ese módulo, notifica a los suscriptores afectados para que renueven en un dispositivo admitido y revoca los certificados que sigan vigentes al cumplirse ese plazo.

La extensión QCStatement de los certificados de los suscriptores identifica el tipo de dispositivo criptográfico conforme al Anexo IV de la Resolución SICYT N° 11/2025 ([OID que determine el Ente Licenciante para el módulo del dispositivo]).

6.3. Otros aspectos de administración de claves

6.3.1. Archivo permanente de la clave pública

Los certificados emitidos a los suscriptores, a los Oficiales de Registro y al respondedor OCSP, y el certificado de la AC EGREGOR, se almacenan en formato DER y se publican bajo un esquema de redundancia, con respaldo periódico, durante al menos diez (10) años desde su vencimiento o revocación. Las políticas y controles para recuperar la clave pública archivada, incluidos el software y el hardware necesarios, se describen en el Plan de Contingencia.

6.3.2. Período de uso de clave pública y privada

Las claves privadas correspondientes a los certificados emitidos pueden ser utilizadas por los suscriptores únicamente durante el período de validez de sus certificados. Las claves públicas pueden utilizarse durante el período establecido por las normas legales vigentes, para verificar las firmas generadas durante el período de validez.

Certificado	Período de validez
AC EGREGOR	Hasta [10] años, sin exceder el del certificado de la AC-RAÍZ
Respondedor OCSP	Hasta 1 año
Personas humanas	2 años
Personas jurídicas	2 años
Oficiales de Registro	Según la política del certificador que los emita

6.4. Datos de activación

Egregor Labs establece medidas de seguridad suficientes para proteger los datos de activación requeridos para operar los dispositivos criptográficos.

6.4.1. Generación e instalación de datos de activación

Los datos de activación de la clave de la AC se generan durante la ceremonia inicial y se distribuyen entre los cinco (5) custodios del control M de N.

Los datos de activación de la clave del suscriptor son su biometría registrada en el dispositivo (Face ID o Touch ID) y su contraseña de firma, de al menos seis (6) caracteres, que el suscriptor define en la aplicación habilitada al generar la clave y que el módulo criptográfico exige junto con la biometría en cada uso. La contraseña de firma es distinta de la contraseña de la cuenta y no puede cambiarse sin generar una clave y un certificado nuevos; si el suscriptor la olvida, la clave queda inutilizable y corresponde la revocación del certificado y la emisión de uno nuevo. El código de desbloqueo no activa la clave ni reemplaza a la biometría ni a la contraseña de firma: es condición para que la clave exista (si se elimina, la clave se borra) y para rehabilitar la biometría después de intentos fallidos. Quien conozca el código tampoco puede registrar una biometría nueva y usar la clave, porque la clave queda inutilizable ante cualquier cambio de la biometría registrada. Egregor Labs no conoce ni almacena ninguno de estos datos, y la aplicación habilitada no guarda la contraseña de firma. La aplicación habilitada no permite generar claves en un dispositivo sin código de desbloqueo y sin biometría configurados. Egregor Labs recomienda en el Acuerdo con Suscriptores usar un código de desbloqueo de al menos seis (6) dígitos o alfanumérico, que no sea fácilmente deducible.

6.4.2. Protección de los datos de activación

Los custodios guardan sus credenciales en sobres lacrados en el nivel 6 de seguridad física y no pueden delegarlas. Los Oficiales de Registro y los suscriptores son responsables de la custodia de su token o dispositivo y de no divulgar su contraseña o código, ni de registrar en el dispositivo la biometría de otra persona. Egregor Labs no implementa mecanismos de respaldo de los datos de activación de Oficiales de Registro ni de suscriptores.

6.4.3. Otros aspectos referidos a los datos de activación

La contraseña de la cuenta en la aplicación habilitada no activa la clave privada: solo da acceso a la cuenta.

6.5. Controles de seguridad informática

6.5.1. Requisitos técnicos específicos

Los requisitos de seguridad del equipamiento y del software de Egregor Labs, detallados en el Manual de Procedimientos y en el Plan de Seguridad, comprenden:

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, con doble factor.
d) Utilización de criptografía en las sesiones de comunicación (TLS 1.2 o superior) y en las bases de datos (cifrado con claves gestionadas en el HSM).
e) Archivo de datos históricos y de auditoría del Certificador y de los usuarios.
f) Registro de eventos de seguridad.
g) Pruebas de seguridad de los servicios de certificación.
h) Mecanismos confiables para la identificación de los roles.
i) Mecanismos de recuperación de claves y del sistema de certificación.

Estas funciones se proveen mediante una combinación del sistema operativo, el software de certificación y los controles físicos.

6.5.2. Requisitos de seguridad computacional

Los servidores de la AC se alojan en el recinto exclusivo descripto en el punto 5.1. Los HSM cuentan con certificación FIPS 140 nivel 3 emitida por el NIST [y Common Criteria, si corresponde]. Los tokens de los Oficiales de Registro cuentan con certificación FIPS 140 nivel 2 o superior. Los módulos criptográficos de los dispositivos de los suscriptores cuentan con la certificación del punto 6.2.11. La aplicación habilitada AdES es evaluada al menos una vez por año por un tercero independiente conforme al estándar OWASP MASVS, perfil L2.

6.6. Controles técnicos del ciclo de vida de los sistemas

Egregor Labs mantiene el control de los equipos y de la documentación de configuración del sistema, y registra toda modificación o actualización. El monitoreo de integridad advierte cualquier cambio en los sistemas de la AC, lo identifica y permite comprobar su validez.

6.6.1. Controles de desarrollo de sistemas

El software de AC se homologa antes de su puesta en producción para asegurar que responde a las características declaradas por su proveedor. Los desarrollos propios de Jacobs Comercial S.R.L., incluidas la AR y la aplicación habilitada AdES, siguen las guías de OWASP (ASVS para servicios y MASVS para la aplicación móvil), con revisión de código, pruebas automatizadas y ambientes separados de desarrollo, prueba y producción.

Toda versión de la aplicación habilitada que modifique la generación de claves, la captura de rostro, la atestación o la firma debe ser aprobada por el Responsable de Seguridad antes de su publicación. Egregor Labs fija una versión mínima de la aplicación habilitada y bloquea las solicitudes de versiones anteriores.

6.6.2. Controles de gestión de seguridad

Se documenta y controla la configuración del sistema y toda modificación o actualización, y se implementa un método de detección de modificaciones no autorizadas.

6.6.3. Controles de seguridad del ciclo de vida del software

Los resultados de las evaluaciones de terceros sobre la aplicación habilitada y sobre la infraestructura se conservan y se ponen a disposición del Ente Licenciante y de los auditores.

6.7. Controles de seguridad de red

La red de la AC está aislada de otras redes y no es accesible directamente desde Internet. Los servicios de la AR, el repositorio y el OCSP se ubican en zonas separadas por cortafuegos ("firewalls") que filtran el tráfico. El acceso administrativo remoto solo se admite mediante una red privada virtual con autenticación de doble factor. La infraestructura de la AC no comparte servidores ni redes con los servicios de la aplicación habilitada que no forman parte de la certificación. Los análisis de seguridad de red se realizan como mínimo cada seis (6) meses.

6.8. Servicios de emisión de sellos de tiempo

No aplica. Egregor Labs no presta el servicio de emisión de sellos de tiempo. Las firmas que produce la aplicación habilitada AdES incorporan un sello de tiempo emitido por una Autoridad de Sello de Tiempo externa, a la que la Autoridad de Registro envía solo la huella criptográfica del valor de cada firma, nunca el documento.

6.9. Servicio de emisión de sello de competencia o atributo

No aplica. Egregor Labs no presta el servicio de emisión de sellos de competencia o atributo.

7. Perfiles de certificados y de listas de certificados revocados

Todos los certificados emitidos bajo esta Política respetan la especificación ITU-T X.509 (ISO/IEC 9594-8), adoptada como estándar tecnológico para la Infraestructura de Firma Digital de la República Argentina, y el Anexo IV de la Resolución SICYT N° 11/2025 ("Perfiles de los Certificados y de las Listas de Certificados Revocados"). Se aplican además los RFC 5280, RFC 3739 y RFC 5480.

7.1. Perfil del certificado

Todos los certificados se emiten conforme a la especificación ITU X.509 versión 3 o la que, en su defecto, determine el Ente Licenciante, y cumplen el apartado 2 del Anexo IV. Bajo esta Política se emiten certificados de: (a) persona humana; (b) persona jurídica; y (c) respondedor OCSP de la AC EGREGOR.

Nombre distintivo del emisor (común a todos los certificados). Coincide con el campo "subject" del certificado de la AC EGREGOR emitido por la AC-RAÍZ. El atributo "organizationName" contiene la razón social del Certificador, no su nombre de fantasía:

Atributo	OID	Valor
commonName	2.5.4.3	AC EGREGOR
serialNumber	2.5.4.5	CUIT 30-71902710-1
organizationName	2.5.4.10	Jacobs Comercial S.R.L.
stateOrProvinceName	2.5.4.8	Ciudad Autónoma de Buenos Aires
countryName	2.5.4.6	AR

Perfil del certificado de persona humana

Campo o extensión	OID	Crítica	Valor
version			2 (versión 3)
serialNumber			Número único asignado por la AC EGREGOR, de al menos 64 bits aleatorios
signature	1.2.840.10045.4.3.3		ecdsa-with-SHA384
issuer			Nombre distintivo del emisor
validity			notBefore: fecha y hora de emisión. notAfter: fecha y hora de emisión + 2 años, sin exceder el vencimiento del certificado de la AC EGREGOR
subject: commonName	2.5.4.3		Nombre y apellido según el DNI
subject: serialNumber	2.5.4.5		“CUIL” o “CUIT” seguido del número
subject: countryName	2.5.4.6		AR
subjectPublicKeyInfo	1.2.840.10045.2.1		id-ecPublicKey, curva secp256r1 (1.2.840.10045.3.1.7)
authorityKeyIdentifier	2.5.29.35	No	Identificador de la clave de la AC EGREGOR
subjectKeyIdentifier	2.5.29.14	No	Resumen SHA-1 de la clave pública del suscriptor
basicConstraints	2.5.29.19	Sí	Subject Type = End Entity; Path Length Constraint = None
keyUsage	2.5.29.15	Sí	digitalSignature, nonRepudiation, keyEncipherment, dataEncipherment y keyAgreement = 1; keyCertSign y cRLSign = 0
extKeyUsage	2.5.29.37	No	id-kp-clientAuth (1.3.6.1.5.5.7.3.2); id-kp-emailProtection (1.3.6.1.5.5.7.3.4)

Campo o extensión	OID	Crítica	Valor
subjectAltName	2.5.29.17	No	rfc822Name: dirección de correo electrónico verificada del suscriptor
cRLDistribution Points	2.5.29.31	No	https:// advancedelectronicsignature.com/crl/ac-egregor.crl y https://[dominio alternativo]/crl/ac-egregor.crl
certificatePolicies	2.5.29.32	No	Policy Identifier: [OID de esta Política]. CPS: https://advancedelectronicsignature.com/politicas/puc.pdf. userNotice: “certificado emitido por un Certificador Licenciado en el marco de la Ley Nº 25.506”
authorityInfoAccess	1.3.6.1.5.5.7.1.1	No	id-ad-ocsp: https://ocsp.advancedelectronicsignature.com; id-ad-caIssuers: https://advancedelectronicsignature.com/ac-egregor.crt
qcStatements	1.3.6.1.5.5.7.1.3	No	[OID del Anexo IV, punto 2.3.11, que corresponda al módulo criptográfico del dispositivo, según el punto 6.2.11]

Perfil del certificado de persona jurídica

Campo o extensión	OID	Crítica	Valor
version, serialNumber, signature, issuer			Iguales al certificado de persona humana
validity			2 años, sin exceder el vencimiento del certificado de la AC EGREGOR
subject: commonName	2.5.4.3		Denominación de la persona jurídica o nombre de la unidad operativa responsable
subject: organizationalUnitName	2.5.4.11		Optativo: unidades operativas relacionadas con el suscriptor (una o más instancias)
subject: organizationName	2.5.4.10		Denominación de la persona jurídica
subject: serialNumber	2.5.4.5		“CUIT” seguido del número, o “ID [país]” seguido del número de identificación tributaria para personas jurídicas extranjeras
subject: countryName	2.5.4.6		AR
subjectPublicKeyInfo	1.2.840.1004		id-ecPublicKey, curva secp256r1

Campo o extensión	OID	Crítica	Valor
	5.2.1		
authorityKeyIdentifier, subjectKeyIdentifier, basicConstraints, keyUsage, extKeyUsage			Iguales al certificado de persona humana
subjectAltName	2.5.29.17	No	Campos “otherName” con los datos de la persona humana a cargo de la custodia de la clave: commonName (2.5.4.3) con su nombre y apellido; serialNumber (2.5.4.5) con “CUIL” o “CUIT” y su número; y title (2.5.4.12) con su cargo o función en la persona jurídica
cRLDistributionPoints, certificatePolicies, authorityInfoAccess, qcStatements			Iguales al certificado de persona humana

Perfil del certificado del respondedor OCSP

Campo o extensión	Valor
subject	CN = OCSP AC EGREGOR, O = Jacobs Comercial S.R.L., serialNumber = CUIT 30-71902710-1, C = AR
subjectPublicKeyInfo	id-ecPublicKey, curva secp384r1 (1.3.132.0.34)
validity	Hasta 1 año
keyUsage (crítica)	digitalSignature, nonRepudiation
extKeyUsage	id-kp-OCSPSigning (1.3.6.1.5.5.7.3.9)
id-pkix-ocsp-nocheck	1.3.6.1.5.5.7.48.1.5, presente
Demás extensiones	authorityKeyIdentifier, subjectKeyIdentifier, basicConstraints (End Entity), certificatePolicies y cRLDistributionPoints, como en los certificados de suscriptores

7.1.1. Número de versión

Los certificados son X.509 versión 3: el campo “version” tiene el valor 2.

7.1.2. Extensiones

Todos los certificados incluyen las extensiones obligatorias del punto 2.3 del Anexo IV: BasicConstraints, KeyUsage, CRLDistributionPoints, CertificatePolicies, AuthorityKeyIdentifier y, en los certificados de personas humanas y jurídicas, SubjectAlternativeName y SubjectKeyIdentifier. Se incluyen además AuthorityInformationAccess y QCStatement. No se crean extensiones distintas de las definidas en el Anexo IV. Egregor Labs no usa delta CRL, por lo que no incluye la extensión FreshestCRL.

7.1.3. Identificadores de algoritmos

- Firma de certificados, CRL y respuestas OCSP: ecdsa-with-SHA384 (1.2.840.10045.4.3.3), conforme al RFC 5758.
- Claves públicas: id-ecPublicKey (1.2.840.10045.2.1) con las curvas secp256r1 (1.2.840.10045.3.1.7) para suscriptores y secp384r1 (1.3.132.0.34) para la AC EGREGOR y el respondedor OCSP, conforme al RFC 5480.

7.1.4. Formatos de nombre

Los nombres distintivos del emisor y del suscriptor se codifican según el punto 3.1 de esta Política y el punto 2.2.6 del Anexo IV, en UTF8String, salvo countryName y serialNumber, en PrintableString.

7.1.5. Restricciones de nombre

No se usa la extensión NameConstraints.

7.1.6. OID de la Política Única de Certificación

[OID asignado por la DNFDIT], incluido en la extensión CertificatePolicies de todos los certificados.

7.1.7. Sintaxis y semántica de calificadores de política

La extensión CertificatePolicies incluye dos calificadores: el calificador CPS, con la URI donde está publicada esta Política, y el calificador userNotice, con la leyenda “certificado emitido por un Certificador Licenciado en el marco de la Ley Nº 25.506”.

7.1.8. Semántica de procesamiento para extensiones críticas

Son críticas las extensiones BasicConstraints y KeyUsage. Toda aplicación que procese un certificado y no reconozca una extensión marcada como crítica debe rechazarlo.

7.2. Perfil de la lista de certificados revocados

Las listas de certificados revocados se emiten conforme a la especificación ITU X.509 versión 2 o la que, en su defecto, determine el Ente Licenciante, y cumplen el apartado 3 del Anexo IV.

Campo o extensión	OID	Crítica	Valor
version			1 (versión 2)
signature	1.2.840.10045.4.3.3		ecdsa-with-SHA384
issuer			Nombre distintivo del emisor del punto 7.1
thisUpdate			Fecha y hora de emisión
nextUpdate			Fecha y hora de emisión + 24 horas
revokedCertificates			Para cada certificado revocado: serialNumber y revocationDate

Campo o extensión	OID	Crítica	Valor
reasonCode (por entrada)	2.5.29.21	No	Motivo de revocación, cuando se conoce
invalidityDate (por entrada)	2.5.29.24	No	Fecha en que se sabe o se sospecha que la clave fue comprometida, cuando corresponde
authorityKeyIdentifier	2.5.29.35	No	Identificador de la clave de la AC EGREGOR
cRLNumber	2.5.29.20	No	Número de secuencia creciente

7.2.1. Número de versión

Las CRL son X.509 versión 2: el campo “version” tiene el valor 1.

7.2.2. Extensiones de CRL

Todas las CRL incluyen las extensiones AuthorityKeyIdentifier y CRLNumber. Egregor Labs emite una única CRL completa, no indirecta, por lo que no usa las extensiones DeltaCRLIndicator, IssuingDistributionPoint, FreshestCRL ni CertificateIssuer. Las entradas incluyen ReasonCode y, cuando corresponde, InvalidityDate.

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

La consulta en línea del estado de un certificado se realiza con el protocolo OCSP, implementado conforme al RFC 6960 y al apartado 4 del Anexo IV.

7.3.1. Consultas OCSP

Las consultas contienen la versión, el requerimiento de servicio, el identificador del certificado consultado y, opcionalmente, extensiones (por ejemplo, un “nonce”). Al recibir la consulta, el respondedor determina si el formato es adecuado, si está habilitado para responderla y si contiene la información necesaria. Si alguna de estas condiciones no se cumple, devuelve un mensaje de error; en caso contrario, devuelve una respuesta. El servicio acepta consultas por HTTP mediante los métodos GET y POST.

7.3.2. Respuestas OCSP

Todas las respuestas son firmadas digitalmente por el respondedor OCSP de la AC EGREGOR, con un certificado emitido por la AC EGREGOR para tal fin, y contienen: la versión de la sintaxis de respuesta; el identificador del respondedor; la fecha y hora de generación; la respuesta sobre el estado del certificado; las extensiones opcionales; el identificador del algoritmo de firma (ecdsa-with-SHA384); y la firma.

Para cada certificado consultado, la respuesta contiene su identificador, el valor de estado, el período de validez de la respuesta (thisUpdate y nextUpdate) y extensiones opcionales. Los valores de estado son:

- **Válido (good):** no existe un certificado con el número de serie consultado que haya sido revocado durante su vigencia.
- **Revocado (revoked):** el certificado fue revocado; se indican la fecha y, cuando se conoce, el motivo.
- **Desconocido (unknown):** el respondedor no reconoce el número de serie, por lo general porque el emisor es desconocido.

El servicio OCSP refleja una revocación inmediatamente después de procesada.

8. Auditoría de cumplimiento y otras evaluaciones

Jacobs Comercial S.R.L., en su carácter de certificador licenciado, está sujeta a las auditorías del artículo 33 y siguientes de la Ley N° 25.506 y de los artículos 6° y 7° del Anexo al Decreto N° 182/2019: la auditoría previa al otorgamiento de la licencia, las auditorías anuales y las que disponga el Ente Licenciante. Estas auditorías verifican el cumplimiento de los requisitos para obtener y mantener la licencia y la aplicación de las políticas y procedimientos aprobados.

Los temas principales a evaluar son:

- Requisitos legales generales.
- Política Única de Certificación y Manual de Procedimientos.
- Plan de Seguridad.
- Plan de Cese de Actividades.
- Plan de Contingencia.
- Plataforma tecnológica.
- Ciclo de vida de las claves criptográficas del Certificador.
- Ciclo de vida de los certificados de los suscriptores, incluidos la validación de identidad con el RENAPER y la verificación de la atestación de la aplicación.
- Estructura y contenido de los certificados y de las CRL.
- Mecanismos de acceso a la documentación publicada, a los certificados y a las CRL.

Además, Egregor Labs realiza:

- Una auditoría interna anual de los procesos de la AC y de la AR CENTRAL.
- Una evaluación anual de la aplicación habilitada AdES por un tercero independiente, conforme al punto 6.5.2.
- Una prueba de penetración anual de la infraestructura y los análisis de red del punto 6.7.

Ante observaciones de las auditorías, una vez notificadas, Egregor Labs adopta las medidas correctivas de carácter legal y técnico que correspondan, con un plan de acción y plazos que informa al Ente Licenciante.

En cumplimiento del artículo 21, inciso k) de la Ley N° 25.506, la información relevante de los informes de la última auditoría se publica según el punto 2.2.

9. Aspectos legales y administrativos

9.1. Aranceles

El certificado y el uso del servicio de firma de la aplicación habilitada AdES se distinguen así:

- **El certificado** se emite, con una validez de dos (2) años, a todo solicitante que cumpla los requisitos de esta Política, sin cargo por la emisión.
- **Firmar con la aplicación habilitada AdES** requiere tener firmas de prueba disponibles o un plan vigente.

Plan	Alcance	Arancel
Prueba	Cinco (5) firmas por persona, por única vez	Sin cargo
Persona humana, anual	Firmas ilimitadas durante doce (12) meses, con renovación automática	Según lo publicado en el sitio web
Persona humana, dos años	Firmas ilimitadas durante veinticuatro (24) meses	Según lo publicado en el sitio web
Persona jurídica, anual	Firmas ilimitadas durante doce (12) meses	Según lo publicado en el sitio web
Convenio con entidades profesionales	Plan anual bonificado total o parcialmente	Según el convenio
Sector Público	Firmas ilimitadas	Sin cargo

Los planes los contrata el suscriptor con Jacobs Comercial S.R.L., que los factura. Los aranceles vigentes, con IVA incluido, los medios de pago y las condiciones de cada convenio se publican en https://advancedelectronicsignature.com/aranceles y en la aplicación habilitada antes de cada contratación. Egregor Labs puede actualizar los aranceles; las actualizaciones rigen para las contrataciones y renovaciones posteriores a su publicación y no afectan los planes ya pagados. Los planes de personas humanas se contratan desde la aplicación habilitada; los de personas jurídicas, con facturación directa de Jacobs Comercial S.R.L. El plan corresponde a la persona titular y vale para todos sus certificados vigentes.

El certificado no se revoca por falta de pago ni por el vencimiento del plan: en ese caso, el suscriptor no puede firmar con la aplicación habilitada hasta contratar un plan, y conserva la posibilidad de verificar firmas, consultar el estado de su certificado y revocarlo.

Son gratuitos, además: la revocación; la consulta de la CRL, del servicio OCSP y del estado de los certificados; el acceso al repositorio; y la sustitución de un certificado revocado porque los procedimientos de emisión o verificación dejaron de ser seguros, conforme al artículo 21, inciso 15 del Anexo al Decreto N° 182/2019.

Los certificados y el servicio de firma para entidades y jurisdicciones del Sector Público se proveen en forma gratuita.

9.2. Responsabilidad financiera

La responsabilidad de Jacobs Comercial S.R.L. por los daños que puedan sufrir los suscriptores y los terceros usuarios por el incumplimiento de las normas legales y reglamentarias y de esta Política se rige por el artículo 38 de la Ley N° 25.506:

“El certificador que emita un certificado digital o lo reconozca en los términos del artículo 16 de la presente ley, 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. Corresponderá al prestador del servicio demostrar que actuó con la debida diligencia.”

Para garantizar el cumplimiento de sus obligaciones, Jacobs Comercial S.R.L. mantiene un seguro de caución a favor de la Autoridad de Aplicación, conforme a los artículos 34 y 35 del Anexo al Decreto N° 182/2019 y al artículo 41 del Anexo I de la Resolución SICYT N° 11/2025, por el monto mínimo que fija el Anexo VII de esa resolución, emitido por [aseguradora], póliza N° [●], vigente mientras subsistan sus obligaciones. [Si se contrata un seguro de responsabilidad civil, indicar aseguradora, póliza y cobertura.]

9.3. Confidencialidad

Todos los datos de las personas humanas y jurídicas alcanzadas por esta Política están sujetos a la Ley N° 25.326 de Protección de los Datos Personales.

9.3.1. Información confidencial

Toda información remitida por el solicitante o suscriptor al efectuar un requerimiento es confidencial y no se divulga a terceros sin su consentimiento previo y expreso, salvo que sea requerida mediante resolución fundada en causa judicial por juez competente o por autoridad administrativa competente en el marco de un procedimiento administrativo. La exigencia se extiende a toda otra información sobre los suscriptores a la que tengan acceso Egregor Labs o la AR CENTRAL durante el ciclo de vida del certificado.

En particular, es confidencial, en la medida en que no sea de conocimiento público:

- Toda la información remitida por el solicitante o suscriptor, excepto los datos que figuran en el certificado: las capturas de rostro y huellas, el resultado del cotejo del RENAPER, la documentación de las personas jurídicas, los datos de contacto y la información técnica del dispositivo.
- La información almacenada en los servidores y bases de datos de la AC y de la AR.
- La parte reservada del Manual de Procedimientos, el Plan de Seguridad, el Plan de Contingencia, los registros de auditoría y los datos de activación.
- La clave privada de la AC EGREGOR, que se genera y custodia conforme a esta Política.

Egregor Labs no tiene acceso a las claves privadas de los suscriptores, que se generan y permanecen en el módulo criptográfico de sus dispositivos, y no genera, almacena, copia ni conserva información que permita reconstruirlas o activarlas.

Egregor Labs solo hace públicos los datos del suscriptor imprescindibles para el reconocimiento de su firma digital, que son los contenidos en el certificado.

9.3.2. Información no confidencial

No se considera confidencial:

a) El contenido de los certificados y de las listas de certificados revocados.
b) La información sobre personas humanas o jurídicas disponible en certificados o en directorios de acceso público.
c) Esta Política y la parte pública del Manual de Procedimientos.
d) Las secciones públicas del Plan de Seguridad.
e) La Política de Privacidad.
f) El Acuerdo con Suscriptores.
g) Los Términos y Condiciones con Terceros Usuarios.

9.3.3. Responsabilidades de los roles involucrados

Todas las personas con roles de confianza firman un acuerdo de confidencialidad antes de acceder a información confidencial, acceden solo a la información necesaria para su función y responden por su divulgación no autorizada. Las responsabilidades de cada rol se describen en el Manual de Procedimientos y en el Plan de Seguridad.

9.4. Privacidad

Todos los aspectos vinculados a la privacidad de los datos personales se rigen por la Ley N° 25.326 y sus normas reglamentarias, complementarias y aclaratorias. Las consideraciones particulares se incluyen en la Política de Privacidad.

9.5. Derechos de propiedad intelectual

Jacobs Comercial S.R.L. es titular exclusiva de los derechos de propiedad intelectual sobre esta Política, el Manual de Procedimientos, los acuerdos, los procedimientos y los demás documentos de su Autoridad Certificante, y sobre los contenidos de su sitio web. La aplicación habilitada “Advanced Electronic Signature” (AdES), su código fuente y las marcas y nombres “Egregor Labs”, “Advanced Electronic Signature” y “AdES” son de titularidad de Jacobs Comercial S.R.L. [indicar los números de solicitud o registro ante el INPI, si corresponde]. Los sistemas operativos y el software de terceros se usan bajo sus respectivas licencias.

Los certificados emitidos y las CRL pueden ser reproducidos libremente para verificar firmas digitales.

9.6. Responsabilidades y garantías

I) Responsabilidades. Conforme al Capítulo IX de la Ley N° 25.506:

a) **Entre Jacobs Comercial S.R.L. y el suscriptor.** Sin perjuicio de la ley y de la legislación vigente, la relación entre Jacobs Comercial S.R.L. y el titular de un certificado

se rige por el Acuerdo con Suscriptores, publicado en https://advancedelectronicsignature.com/firma-digital.

b) **De Jacobs Comercial S.R.L. ante terceros usuarios.** Jacobs Comercial S.R.L. responde en los términos del artículo 38 de la Ley N° 25.506 transcripto en el punto 9.2.

Jacobs Comercial S.R.L. responde por los actos de su Autoridad de Registro y de los terceros que le prestan servicios de infraestructura tecnológica, conforme a los artículos 20 y 32 del Anexo al Decreto N° 182/2019.

II) Garantías.

a) **De Egregor Labs:** que no existen distorsiones en la información contenida en los certificados ni en su emisión; que no existen errores en la información introducida por quien aprobó la emisión; y que los certificados cumplen los requisitos de esta Política.
b) **De la AR CENTRAL:** que no existen distorsiones en la información de los certificados; que no existen errores en la información verificada por ella; y que los dispositivos y la aplicación habilitada cumplen lo dispuesto en esta Política.
c) **Del suscriptor:** que cada firma digital creada con su clave privada corresponde a la clave pública del certificado; que su clave privada está protegida y que no autoriza a otras personas a usarla; que toda la información que facilitó y que contiene el certificado es verdadera; y que usa el certificado exclusivamente para los fines autorizados.
d) **De los terceros usuarios:** que han obtenido información suficiente para decidir si confían en el certificado, verificando su validez y su estado.

9.7. Deslinde de responsabilidad

Conforme al artículo 39 de la Ley N° 25.506, Jacobs Comercial S.R.L. no es responsable:

a) Por los casos que se excluyan taxativamente en las condiciones de emisión y utilización de sus certificados y que no estén expresamente previstos en la ley.
b) Por los daños y perjuicios que resulten del uso no autorizado de un certificado digital, si en las condiciones de emisión y utilización constan las restricciones de su utilización.
c) Por eventuales inexactitudes en el certificado que resulten de la información facilitada por el titular que, según las normas y el Manual de Procedimientos, deba ser objeto de verificación, siempre que Egregor Labs pueda demostrar que tomó todas las medidas razonables.

En particular, y siempre dentro de esos límites:

- **Egregor Labs y la AR CENTRAL** no responden por los daños derivados de la pérdida del control exclusivo del suscriptor sobre su dispositivo, su biometría, su contraseña de firma o su código de desbloqueo, ni del uso de un dispositivo modificado en contra del punto 4.5.1.b), ni por la falta de verificación de la validez de un certificado por parte de los terceros usuarios.
- **El suscriptor** no responde por las firmas producidas con su certificado después de haber solicitado su revocación por las vías del punto 3.4.
- **Los terceros usuarios** asumen las consecuencias de confiar en un certificado sin verificar su validez y su estado en el momento de la firma.

Los tipos de daño cubiertos son los daños directos que resulten de los supuestos del artículo 38 de la Ley N° 25.506.

9.8. Limitaciones a la responsabilidad frente a terceros

Las limitaciones de responsabilidad frente a los terceros usuarios son las del punto 9.7 y se detallan en los Términos y Condiciones con Terceros Usuarios. Dentro de los límites de la normativa vigente, el Acuerdo con Suscriptores establece las limitaciones de responsabilidad de los suscriptores y de Jacobs Comercial S.R.L., que excluyen los daños indirectos, especiales, incidentales y derivados.

9.9. Compensaciones por daños y perjuicios

Las compensaciones se rigen por la Ley N° 25.506 y el derecho común. Egregor Labs no establece compensaciones adicionales a las legales.

9.10. Condiciones de vigencia

I) Entrada en vigencia. Esta Política entra en vigencia al publicarse en el sitio web de Egregor Labs, previa aprobación del Ente Licenciante. Desde ese momento, todos los nuevos certificados se emiten conforme a ella.

II) Finalización. Esta Política está vigente hasta que se derogue expresamente por la entrada en vigencia de una nueva versión aprobada.

III) Consecuencias de la finalización. Los certificados emitidos bajo esta Política siguen vigentes hasta su expiración o revocación, salvo que la nueva versión disponga, por razones críticas de seguridad, su revocación inmediata, en cuyo caso se aplica el artículo 21, inciso 15 del Anexo al Decreto N° 182/2019.

9.11. Avisos personales y comunicaciones con los participantes

No aplicable.

9.12. Gestión del ciclo de vida del documento

Esta Política contempla las siguientes fases: planificación, en la que se identifican las necesidades de cambio; evaluación, en la que se analizan su impacto técnico, operativo y legal; aprobación interna, por el Responsable de la AC y la Gerencia de Jacobs Comercial S.R.L.; aprobación del Ente Licenciante; publicación en el sitio web; y puesta en vigencia.

9.12.1. Procedimientos de cambio

Egregor Labs revisa esta Política y sus documentos complementarios al menos una vez por año, para corregir faltas de claridad y adaptarlos a cambios en la normativa, en la tecnología de los dispositivos admitidos o en sus procesos. Toda modificación se somete a la aprobación previa del Ente Licenciante, conforme al artículo 21, inciso q) de la Ley N° 25.506, al Decreto N° 182/2019 y sus modificatorios y a la Resolución SICYT N° 11/2025. Cada nueva versión describe los cambios respecto de la anterior.

La actualización del listado de dispositivos y versiones admitidos del punto 2.2.k), cuando solo refleja cambios en el estado de certificación publicado por el NIST, no constituye una modificación de esta Política.

9.12.2. Mecanismo y plazo de publicación y notificación

La versión vigente y las anteriores están disponibles en forma permanente en https://advancedelectronicsignature.com/politicas. Ante modificaciones sustanciales, los suscriptores con certificados vigentes son notificados en la aplicación habilitada y por correo electrónico antes de su entrada en vigencia.

9.12.3. Condiciones de modificación del OID

No aplicable.

9.13. Procedimientos de resolución de conflictos

En ningún caso esta Política prevalece sobre la normativa vigente de firma digital.

Ante cualquier discrepancia o conflicto sobre la interpretación o aplicación de esta Política o de los acuerdos en que Jacobs Comercial S.R.L. sea parte, el interesado presenta un reclamo escrito a Egregor Labs, por correo electrónico a reclamos@advancedelectronicsignature.com o en su domicilio, conforme al artículo 17 del Anexo I de la Resolución SICYT N° 11/2025. Egregor Labs:

1. Labra un acta con los hechos que motivan el reclamo y sus antecedentes.
2. Da traslado del acta a las partes involucradas (AR CENTRAL, suscriptor o tercero usuario), que disponen de diez (10) días corridos para ofrecer y producir prueba y alegar.
3. Resuelve dentro de los diez (10) días corridos siguientes, conforme a criterios de razonabilidad, equidad y ajuste a la normativa vigente, y notifica la resolución.

Agotado este procedimiento, el suscriptor o el tercero usuario puede accionar ante la Autoridad de Aplicación, sin perjuicio de su derecho a acudir a la vía judicial.

Los registros electrónicos almacenados en condiciones de seguridad razonables y grabados sistemáticamente en un medio inalterable constituyen evidencia del cumplimiento de las obligaciones de Egregor Labs y de su Autoridad de Registro, y de las comunicaciones, aceptaciones y pagos entre las partes.

9.14. Legislación aplicable

La legislación que respalda la interpretación, aplicación y validez de esta Política es la Ley N° 25.506 y su modificatoria, el Decreto N° 182/2019 y sus modificatorios, el Decreto N° 743/2024, la Resolución SICYT N° 11/2025 y la normativa complementaria.

9.15. Conformidad con normas aplicables

Son aplicables a la actividad de Jacobs Comercial S.R.L., además de la normativa del punto 9.14, la Ley N° 25.326 de Protección de los Datos Personales y sus normas reglamentarias, la Ley

General de Sociedades N° 19.550, y la Ley N° 24.240 de Defensa del Consumidor en lo que corresponda a los suscriptores que sean consumidores.

9.16. Cláusulas adicionales

No se establecen cláusulas adicionales.

9.17. Otras cuestiones generales

Si alguna disposición de esta Política fuera declarada inválida, las restantes conservan su validez. Jacobs Comercial S.R.L. publica el certificado de clave pública de la AC EGREGOR en el Boletín Oficial durante un (1) día, conforme al artículo 21, inciso 13 del Anexo al Decreto N° 182/2019.