Acuerdo con Suscriptores

Egregor Labs S.A. — Versión 1.0 — Fecha: [●]

Contenidos conforme al Anexo V de la Resolución SICYT N° 11/2025.

Introducción

El presente acuerdo entre Egregor Labs S.A. ("Egregor Labs") y el suscriptor o titular de un certificado digital determina los derechos y obligaciones de las partes respecto de la solicitud, aceptación y uso de los certificados de firma digital emitidos conforme a la Política Única de Certificación de Egregor Labs ("la Política"), aprobada por [acto administrativo], disponible en https://firmadigitalapp.com.ar/politicas.

El suscriptor celebra este acuerdo desde la aplicación habilitada "Firma Digital Argentina": lo acepta antes de la emisión de su certificado y, al recibirlo, lo firma digitalmente con él. Esa firma digital equivale a su firma manuscrita (artículo 3 de la Ley N° 25.506), constituye además la aceptación del certificado, y Egregor Labs conserva el acuerdo firmado en el legajo del suscriptor.

1. Solicitud de certificado

1.1. Descripción de los certificados

Los certificados emitidos bajo la Política pueden ser utilizados por sus titulares para firmar digitalmente cualquier documento o transacción, y para autenticación o cifrado. Algunos terceros pueden exigir un medio de almacenamiento determinado o limitar el ámbito de uso de los certificados que aceptan.

La vigencia de todos los certificados es de dos (2) años. La emisión del certificado no tiene cargo. Para firmar con la aplicación habilitada, el suscriptor necesita firmas de prueba disponibles o un plan vigente, según el punto 9.1 de la Política:

- **Prueba:** cinco (5) firmas sin cargo, por única vez por persona.
- **Planes pagos:** anual con renovación automática, o de dos (2) años, para personas humanas, contratados desde la aplicación a través de la App Store; y anual para personas jurídicas, con facturación directa. Los aranceles vigentes se publican en https://firmadigitalapp.com.ar/aranceles.
- **Convenios** con entidades profesionales y **Sector Público**, según el punto 9.1 de la Política.

El plan corresponde al suscriptor y vale para todos sus certificados vigentes. La suscripción anual se renueva automáticamente hasta que el suscriptor la cancele desde la configuración de su cuenta de Apple, y su reintegro se rige por las condiciones de la App Store. Si el plan vence o

no se paga, el certificado **no** se revoca: el suscriptor no puede firmar con la aplicación habilitada hasta contratar un plan, y puede seguir verificando firmas, consultando el estado de su certificado y revocándolo.

1.2. Generación y uso de las claves

El par de claves se genera en el módulo criptográfico de hardware (Secure Enclave) del dispositivo del suscriptor, mediante la aplicación habilitada. La clave privada:

- se genera y queda dentro del módulo, y no puede ser exportada ni copiada, ni siquiera por el suscriptor;
- solo puede usarse en ese dispositivo, que debe tener un código de desbloqueo configurado, y cada operación requiere juntas la autenticación biométrica (Face ID o Touch ID) de su titular y su contraseña de firma; el código de desbloqueo no reemplaza a ninguna de las dos;
- la contraseña de firma la define el suscriptor al generar la clave, es distinta de la contraseña de su cuenta, no la conoce Egregor Labs ni la guarda la aplicación, y no puede cambiarse sin solicitar un certificado nuevo; si la olvida, la clave queda inutilizable y debe revocar el certificado y solicitar otro;
- queda inutilizable si se agrega o modifica un dato biométrico registrado en el dispositivo;
- nunca es conocida por Egregor Labs, por su Autoridad de Registro ni por ningún tercero.

El certificado solo puede usarse desde el dispositivo en el que se generó la clave. Para firmar desde otro dispositivo, el suscriptor debe solicitar otro certificado desde ese dispositivo.

1.3. Requisitos del dispositivo

El suscriptor debe usar un iPhone que figure en el listado de dispositivos admitidos publicado por Egregor Labs, con una versión de iOS admitida, con código de desbloqueo y biometría configurados, sin modificaciones que alteren sus controles de seguridad (por ejemplo, “jailbreak”) y con la aplicación habilitada obtenida de la tienda oficial y actualizada a la versión mínima exigida.

1.4. Compromisos del suscriptor persona humana

Para que la solicitud, aceptación y uso de su certificado adquieran plena legitimidad y eficacia jurídica, el suscriptor acepta que:

a) Toda la información que suministre a Egregor Labs en la solicitud es veraz.
b) Es la única persona que tiene y tendrá acceso a su clave privada: no registrará en su dispositivo la biometría de otra persona ni compartirá su código de desbloqueo ni su contraseña de firma, y se responsabiliza de que ningún tercero pueda usar su clave.
c) Usará su certificado exclusivamente para propósitos legítimos y autorizados, conforme a este acuerdo y a la Política.
d) Informará a Egregor Labs cualquier cambio en los datos de su certificado y solicitará de inmediato su revocación ante cualquier circunstancia que pueda haber comprometido su clave privada.

1.5. Compromisos del suscriptor persona jurídica

Los certificados de persona jurídica se emiten a favor de una persona jurídica pública o privada, a solicitud de su representante legal o de un apoderado con poder suficiente, para que se usen en representación de la persona jurídica con el alcance del poder o instrumento que otorga esa representación. El representante o apoderado es el responsable de la custodia de la clave, que se genera en su dispositivo.

La persona jurídica y su responsable aceptan que:

a) Toda la información suministrada en la solicitud es veraz.
b) El responsable es la única persona que tiene y tendrá acceso a la clave privada y responde por su custodia.
c) El certificado se usará exclusivamente para propósitos legítimos y autorizados, conforme a este acuerdo y a la Política.
d) Informarán de inmediato a Egregor Labs: el cese en sus funciones del representante legal o la revocación o el vencimiento del poder del apoderado; cualquier cambio en los datos del certificado; el cese de la existencia de la persona jurídica; y cualquier circunstancia que pueda haber comprometido la clave privada, solicitando en todos esos casos la revocación del certificado.

1.6. Conformidad con la información del certificado

Antes de la emisión, la aplicación habilitada muestra al solicitante los datos que contendrá el certificado. Al aceptar este acuerdo, el solicitante presta su conformidad respecto de la veracidad de esa información, y su consentimiento para que Egregor Labs publique el estado de su certificado en la Lista de Certificados Revocados y en el servicio OCSP cuando corresponda.

2. Procesamiento de la solicitud de certificado

2.1. Validación de identidad

La identidad del solicitante se valida, en la emisión, la renovación y, cuando el suscriptor no puede acceder a su dispositivo ni a su cuenta, la revocación, con el servicio de validación de identidad del Registro Nacional de las Personas (RENAPER), conforme al Decreto N° 743/2024 y a la Resolución SICYT N° 11/2025:

- **En forma remota:** desde la aplicación habilitada, con la captura del rostro y una prueba de vida.
- **En forma presencial:** ante un Oficial de Registro de la Autoridad de Registro Central, con captura de rostro y huellas dactilares.

En los certificados de personas jurídicas, un Oficial de Registro verifica además la documentación que acredita la existencia de la persona jurídica y la representación invocada.

2.2. Pasos desde la solicitud hasta la emisión

1. El solicitante valida su identidad y, en su caso, presenta la documentación de la persona jurídica.
2. Confirma los datos del certificado.
3. Genera su par de claves en el dispositivo; la aplicación envía la solicitud de certificado (CSR), firmada con la clave nueva, junto con una atestación de que proviene de la aplicación habilitada.
4. Acepta este acuerdo y elige la prueba gratuita o un plan pago, salvo que ya tenga un plan asignado.
5. La Autoridad de Registro verifica la solicitud y la aprueba o la rechaza. El resultado se informa en la aplicación y por correo electrónico, con el motivo en caso de rechazo. El solicitante puede consultar el estado de su trámite en la aplicación.
6. Egregor Labs emite el certificado y lo entrega en la aplicación, que lo instala.
7. El suscriptor controla los datos del certificado y firma digitalmente este acuerdo con él, lo que constituye la aceptación del certificado.

2.3. Aceptación del certificado

El suscriptor debe controlar el contenido del certificado que la aplicación le muestra. Si es correcto, lo acepta firmando digitalmente este acuerdo con él. Si existiera algún error u omisión, debe rechazarlo desde la aplicación o solicitar su revocación dentro de las cuarenta y ocho (48) horas de la notificación. Ante la ausencia de reclamos en ese plazo se tiene por confirmada la exactitud del contenido y el suscriptor asume todas las obligaciones de la Política; el certificado no puede usarse para firmar otros documentos hasta que este acuerdo esté firmado.

2.4. Renovación

La renovación siempre genera un nuevo par de claves y repite la validación de identidad con el RENAPER. Si el certificado anterior está vigente, la solicitud de renovación se firma con él. En los certificados de personas jurídicas, se presenta nuevamente la documentación. La aplicación avisa treinta (30) días antes del vencimiento.

3. Obligaciones ante la revocación o expiración

3.1. Obligaciones del suscriptor

El suscriptor se compromete a usar su clave privada en forma responsable, conforme a este acuerdo y a la Política, y está obligado a solicitar de inmediato la revocación de su certificado, entre otros, en estos casos:

a) Sospecha de que su clave privada está comprometida.
b) Pérdida, robo o entrega a un tercero de su dispositivo sin haberlo borrado.
c) Modificación de los datos biométricos registrados en su dispositivo, olvido de la contraseña de firma o cualquier otra circunstancia que impida usar la clave, y sospecha de que un tercero conoce su contraseña de firma.

d) Cambios en los datos contenidos en el certificado.
e) En certificados de personas jurídicas: cese en sus funciones del representante legal, revocación o vencimiento del poder del apoderado, o cese de la existencia de la persona jurídica.
f) Cuando la información del certificado o de la solicitud haya dejado de ser válida.

A partir de la expiración o de la notificación de la revocación de su certificado, el suscriptor debe abstenerse de usarlo.

3.2. Cómo solicitar la revocación

La recepción de solicitudes de revocación está disponible los siete (7) días de la semana, las veinticuatro (24) horas. Revocar es simple a propósito: no hace falta ningún código especial, ni Face ID, ni la contraseña de firma. El suscriptor escribe la frase "revocar mi certificado" para confirmar que no lo hace por error:

- **Desde su cuenta**, en la aplicación en cualquier dispositivo o en el portal web https://firmadigitalapp.com.ar/cuenta desde cualquier navegador, con la sesión iniciada. Se procesa de inmediato. Sirve para el certificado del teléfono que está usando y para el de un teléfono perdido o robado. El suscriptor debe proteger el acceso a su cuenta, porque quien acceda a ella puede revocar sus certificados, aunque nunca usarlos.
- **Validando su identidad ante la Mesa de Ayuda** al [●], 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 Autoridad de Registro Central, si no puede acceder a su dispositivo ni a su cuenta. Se procesa dentro de las veinticuatro (24) horas.

Eliminar la cuenta en la aplicación habilitada revoca todos los certificados del suscriptor.

3.3. Obligaciones de Egregor Labs

Egregor Labs se obliga a:

a) Revocar el certificado dentro de las veinticuatro (24) horas de recibida una solicitud válida, y de inmediato en las solicitudes desde la cuenta.
b) Publicar la revocación en el servicio OCSP y en la Lista de Certificados Revocados.
c) Notificar la revocación al suscriptor en la aplicación y por correo electrónico, indicando la causa cuando no la haya solicitado él.
d) Revocar el certificado en los demás casos del punto 4.9.1 de la Política, incluidos los que disponga la autoridad judicial o la Autoridad de Aplicación.
e) Sustituir sin cargo el 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.

También pueden solicitar la revocación las personas indicadas en el punto 4.9.2 de la Política.

4. Política de Privacidad

Egregor Labs y su Autoridad de Registro se rigen por la Política de Privacidad publicada en https://firmadigitalapp.com.ar/privacidad, conforme al Anexo VIII de la Resolución SICYT N° 11/2025 y a la Ley N° 25.326.

Egregor Labs recaba únicamente los datos personales necesarios para emitir y gestionar el certificado, y mantiene la confidencialidad de toda la información que no figure en él. La captura de rostro y, en su caso, de huellas se usa solo para validar la identidad con el RENAPER y se conserva como respaldo del trámite. Egregor Labs no envía publicidad al suscriptor por intermedio del servicio de certificación sin su consentimiento expreso.

5. Limitaciones de la responsabilidad

5.1. Fuerza mayor

Ninguna de las partes es responsable por la finalización, interrupción o demora en el cumplimiento de sus obligaciones que resulte de caso fortuito o fuerza mayor (artículo 1730 y concordantes del Código Civil y Comercial de la Nación), siempre que la parte que lo invoque lo haya comunicado a la otra en forma comprobable dentro de las veinticuatro (24) horas de conocido el hecho y haya tomado las medidas razonables para mitigar sus efectos. Se consideran, entre otros, la indisponibilidad de servicios de terceros ajenos al control de las partes, como el servicio de validación de identidad del RENAPER o los servicios del fabricante del dispositivo, sin perjuicio de que Egregor Labs mantiene en todo momento la recepción de revocaciones y la consulta del estado de los certificados conforme a su Plan de Contingencia.

5.2. Casos en que Egregor Labs puede limitar su responsabilidad

Conforme al artículo 39 de la Ley N° 25.506 y al punto 9.7 de la Política, Egregor Labs 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, si en las condiciones de emisión y utilización constan las restricciones de su uso.
c) Por eventuales inexactitudes en el certificado que resulten de la información facilitada por el titular que deba ser objeto de verificación, siempre que Egregor Labs pueda demostrar que tomó todas las medidas razonables.
d) Por los daños derivados de que el suscriptor haya perdido el control exclusivo de su dispositivo, de su biometría, de su contraseña de firma o de su código de desbloqueo, haya usado un dispositivo modificado o no admitido, o no haya solicitado a tiempo la revocación.

Las limitaciones de responsabilidad incluyen la exclusión de daños indirectos, especiales, incidentales y derivados, dentro de los límites de la normativa vigente.

6. Legislación aplicable y procedimientos de resolución de conflictos

Este acuerdo se rige por 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, la Ley N° 25.326 y, supletoriamente, el Código Civil y Comercial de la Nación y la Ley N° 24.240 de Defensa del Consumidor en lo que corresponda.

Ante cualquier discrepancia, el suscriptor presenta un reclamo escrito a Egregor Labs en reclamos@firmadigitalapp.com.ar o en su domicilio. Egregor Labs labra un acta, da traslado a las partes involucradas, que tienen diez (10) días corridos para ofrecer prueba y alegar, y resuelve dentro de los diez (10) días corridos siguientes. Agotado ese procedimiento, el suscriptor puede recurrir a la Autoridad de Aplicación, sin perjuicio de su derecho a acudir a la vía judicial.

Los registros electrónicos que Egregor Labs conserva en condiciones de seguridad razonables constituyen evidencia del cumplimiento de las obligaciones de las partes, de sus comunicaciones, aceptaciones y pagos, y deben ser sustanciados en el procedimiento que corresponda.

7. Cesión de derechos

Ninguno de los derechos del suscriptor bajo este acuerdo puede ser cedido ni transferido. En particular, el suscriptor no puede permitir el acceso de terceros a su clave privada ni a su dispositivo en condiciones que permitan usarla.

8. Contactos

Servicio de atención	Mesa de Ayuda de Egregor Labs
Correo electrónico	ayuda@firmadigitalapp.com.ar
Teléfono	[●] (revocaciones con validación de identidad, las 24 horas)
Domicilio	[●], Ciudad Autónoma de Buenos Aires

El suscriptor puede solicitar el acceso, la rectificación o la actualización de sus datos personales en privacidad@firmadigitalapp.com.ar, según la Política de Privacidad.

9. Vigencia

Este acuerdo rige desde su aceptación por el suscriptor en la aplicación habilitada y hasta que cese su condición de suscriptor conforme a la Política, por expiración o revocación de todos sus certificados. Las obligaciones de conservación y confidencialidad subsisten después de su finalización.

10. Modificaciones a este acuerdo

Toda modificación de este acuerdo requiere la aprobación previa del Ente Licenciante. Aprobada, se publica en el sitio web y se notifica al suscriptor en la aplicación habilitada y a su correo electrónico verificado, con al menos treinta (30) días de anticipación a su entrada en vigencia. Si el suscriptor no acepta la modificación, puede solicitar la revocación de su certificado; continuar usándolo después de la entrada en vigencia implica su aceptación. Los certificados emitidos siguen rigiéndose por la versión de la Política bajo la cual se emitieron.

11. Consentimiento informado

Declaro que fui informado y entiendo el alcance y las consecuencias legales del uso de la firma digital emitida por Egregor Labs; que una firma digital hecha con mi certificado se presume mía y de mi autoría (artículos 7 y 8 de la Ley N° 25.506); que las explicaciones me fueron dadas en un lenguaje claro y sencillo; y que conozco las obligaciones que asumo en este acuerdo. Tuve la oportunidad de verificar la exactitud de los datos que se incluirán en mi certificado y confirmo que son correctos.

Aceptación. El suscriptor acepta este acuerdo firmándolo digitalmente en la aplicación habilitada con la clave privada correspondiente a la solicitud. En la modalidad presencial, además, puede firmarlo en forma ológrafa ante el Oficial de Registro.

Tipo de certificado: [ ] Persona humana [ ] Persona jurídica