Términos y Condiciones con Terceros Usuarios

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

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

1. Resumen

1.1. Contenido de este documento

Este documento establece los términos y condiciones entre Egregor Labs S.A. (“Egregor Labs”) y los terceros usuarios de los certificados digitales que emite, y determina los derechos y responsabilidades de las partes respecto de la verificación de firmas digitales y de los demás usos de esos certificados.

Los terceros usuarios toman conocimiento y aceptan que Egregor Labs no tiene vínculo contractual con ellos, y que se limitan a usar los servicios de consulta que Egregor Labs presta en el marco de su Política Única de Certificación (“la Política”) y de la normativa vigente.

1.2. Identificación de este documento

Nombre	Términos y Condiciones con Terceros Usuarios de Egregor Labs S.A.
Versión	1.0
Fecha	[●]
Lugar	República Argentina
URL	https://firmadigitalapp.com.ar/politicas/terminos-terceros.pdf

1.3. Información publicada

En https://firmadigitalapp.com.ar/firma-digital, disponible las veinticuatro (24) horas de los siete (7) días de la semana, Egregor Labs publica: la Política vigente y sus versiones anteriores; el Manual de Procedimientos (parte pública); el Acuerdo con Suscriptores; la Política de Privacidad; estos Términos y Condiciones; el certificado de la AC EGREGOR y el acceso al certificado de la Autoridad Certificante Raíz de la República Argentina (AC-RAÍZ); la Lista de Certificados Revocados (CRL); el servicio de consulta del estado de los certificados; el listado de Autoridades de Registro; el listado de dispositivos admitidos; y la información relevante de las auditorías.

2. Definiciones

Rigen las definiciones del punto 1.6 de la Política. En particular:

- **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:** 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 otorgada por el Ente Licenciante (artículo 17 de la Ley N° 25.506). A los efectos de este documento, Egregor Labs.
- **Firma digital:** resultado de aplicar a un documento digital un procedimiento matemático que requiere información de exclusivo conocimiento del firmante, bajo su absoluto control, susceptible de verificación por terceras partes de modo que permita identificar al firmante y detectar cualquier alteración posterior del documento (artículo 2 de la Ley N° 25.506).
- **Lista de Certificados Revocados (CRL):** lista de certificados dejados sin efecto en forma permanente por el certificador, firmada y publicada por él.
- **Servicio OCSP:** servicio de verificación en línea del estado de los certificados, cuyas respuestas firma el certificador.
- **Suscriptor:** persona a cuyo nombre se emite un certificado y que posee la clave privada correspondiente a la clave pública que contiene.
- **Tercero usuario:** persona humana o jurídica que recibe un documento firmado digitalmente y que genera una consulta para verificar la validez del certificado correspondiente.
- **Dispositivo del suscriptor:** iPhone admitido en cuyo módulo criptográfico de hardware se genera y guarda la clave privada del suscriptor, que no puede exportarse y cuyo uso requiere la autenticación biométrica de su titular.

3. Reconocimiento de información suficiente

La Política rige la relación entre Egregor Labs, los suscriptores y los terceros usuarios, y establece las responsabilidades de las partes.

El tercero usuario acepta su obligación de conocer, antes de confiar en un certificado emitido por Egregor Labs: la Política, en particular sus puntos 1.4 (uso de los certificados), 4.5.2 (obligaciones de los terceros usuarios), 4.9 (revocación) y 9.7 (deslinde de responsabilidad); las características de los certificados y de las CRL descriptas en su sección 7; y estos Términos y Condiciones.

En particular, el tercero usuario reconoce que:

- La clave privada del suscriptor se genera en el módulo criptográfico de su teléfono, no puede exportarse y cada uso requiere la autenticación biométrica del titular en ese teléfono.
- La identidad del suscriptor fue validada por Egregor Labs con el RENAPER, en forma remota o presencial.
- En los certificados de personas jurídicas, la extensión “SubjectAlternativeName” identifica a la persona humana que custodia la clave y su cargo o función.

4. Política Única de Certificación

4.1. Tipos de certificados

Bajo la Política se emiten:

- **Certificados de persona humana:** a favor de personas humanas con DNI y CUIL o CUIT, identificadas por su nombre y apellido según el DNI y su CUIL o CUIT. Vigencia: dos (2) años.
- **Certificados de persona jurídica:** a favor de personas jurídicas públicas o privadas, a solicitud de su representante legal o apoderado, identificadas por su denominación y CUIT, con los datos de la persona humana responsable de la custodia de la clave. Vigencia: dos (2) años.

Egregor Labs también emite el certificado de su respondedor OCSP. No emite certificados de aplicaciones, de sitio seguro ni de sellos de tiempo o competencia.

4.2. Aplicabilidad

Las claves correspondientes a los certificados emitidos bajo la Política pueden ser utilizadas en forma interoperable en los procesos de firma digital de cualquier documento o transacción y para la autenticación o el cifrado.

4.3. Limitaciones en el uso del certificado

No existen restricciones en el uso del certificado, excepto las indicadas en la Ley N° 25.506 y su modificatoria, en su Decreto Reglamentario N° 182/2019 y sus modificatorios y en la demás normativa aplicable.

5. Obligaciones de los terceros usuarios

De acuerdo con el punto 4.5.2 de la Política, los terceros usuarios deben:

a) Conocer los alcances de la Política.
b) Verificar la validez del certificado digital.

Para verificar la validez, el tercero usuario debe:

1. Verificar la firma digital del documento con la clave pública del certificado del firmante.
2. Verificar la cadena de confianza: que el certificado del firmante esté firmado por la AC EGREGOR, y que el certificado de la AC EGREGOR esté firmado por la AC-RAÍZ.
3. Verificar que el certificado estuviera vigente en el momento de la firma.
4. Verificar que el certificado no estuviera revocado en el momento de la firma, mediante la CRL vigente (https://firmadigitalapp.com.ar/crl/ac-egregor.crl) o el servicio OCSP (https://ocsp.firmadigitalapp.com.ar), comprobando la firma y la vigencia de la CRL o de la respuesta OCSP.

5. En los certificados de personas jurídicas, considerar el cargo o función del responsable que figura en el certificado.

Si no puede obtener una CRL vigente ni una respuesta OCSP, el tercero usuario debe optar entre rechazar el documento, aceptarlo bajo su exclusiva responsabilidad o postergar la decisión hasta obtener la información de estado.

6. Revocación de los certificados de nivel superior

El tercero usuario está expuesto a los riesgos del compromiso de las claves privadas de nivel superior. Por eso debe verificar también el estado del certificado de la AC EGREGOR y el de la AC-RAÍZ.

Si el certificado de la AC EGREGOR fuera revocado, los certificados que emitió quedarían sin sustento, en una situación equivalente a la revocación, y Egregor Labs no podría emitir nuevos certificados ni CRL con esa clave. Lo mismo ocurriría si se revocara el certificado de la AC-RAÍZ. Ese estado se hace evidente al verificar la cadena de confianza y las CRL de nivel superior según el punto 5.

Ante el compromiso de su clave privada, Egregor Labs revoca todos los certificados emitidos, publica una CRL final, informa al Ente Licenciante y a la AC-RAÍZ, y publica un aviso destacado en su sitio web.

7. Limitaciones de responsabilidad

7.1. Fuerza mayor

Conforme al Código Civil y Comercial de la Nación (artículo 1730 y concordantes), los casos de fuerza mayor o caso fortuito, vinculados a circunstancias ajenas a la voluntad de las partes, no generan derecho a indemnización a favor del damnificado, siempre que la parte que lo invoque haya tomado las medidas razonables para mitigar sus efectos.

7.2. Casos en los cuales el certificador 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 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 deba ser objeto de verificación, siempre que Egregor Labs pueda demostrar que tomó todas las medidas razonables.
d) Por los daños que sufra el tercero usuario que confíe en un certificado sin verificar su validez y su estado conforme al punto 5.

8. Legislación aplicable y procedimientos de resolución de conflictos

8.1. Legislación aplicable

La legislación que respalda la interpretación, aplicación y validez de la Política y de este documento 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 sus normas complementarias. Se aplican también la Ley N° 25.326 y, supletoriamente, el Código Civil y Comercial de la Nación.

8.2. Forma de interpretación y aplicación

Este documento y la Política se interpretan conforme a esa normativa, que prevalece en caso de conflicto.

8.3. Procedimientos de resolución de conflictos

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

La documentación y la información almacenadas por Egregor Labs en condiciones de seguridad razonables y registradas sistemáticamente en un medio inalterable constituyen evidencia del cumplimiento de sus obligaciones, y deben ser sustanciadas en el procedimiento que corresponda.

9. Contactos

Servicio de atención de consultas	Mesa de Ayuda de Egregor Labs
Correo electrónico institucional	ayuda@firmadigitalapp.com.ar
Teléfono	[●]
Domicilio	[●], Ciudad Autónoma de Buenos Aires