Política de Privacidad

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

Contenidos conforme al Anexo VIII de la Resolución SICYT N° 11/2025 y a la Ley N° 25.326.

1. Introducción

Egregor Labs S.A. ("Egregor Labs"), en su condición de certificador licenciado, declara en este documento cómo trata la información que recibe para prestar sus servicios de certificación digital.

2. Identificación de este documento

Nombre	Política de Privacidad de Egregor Labs S.A.
Versión	1.0
Fecha	[●]
Lugar	República Argentina
URL	https://firmadigitalapp.com.ar/privacidad

3. Objeto y alcance

Este documento determina el tratamiento que Egregor Labs da a los datos que recibe de los solicitantes, suscriptores, terceros usuarios y otros terceros en general, en el marco de su Política Única de Certificación ("la Política"), conforme a la Ley N° 25.326 de Protección de los Datos Personales y sus normas complementarias, la Ley N° 25.506 de Firma Digital y la Resolución SICYT N° 11/2025. Alcanza a Egregor Labs y a su Autoridad de Registro Central.

Responsable de la base de datos: Egregor Labs S.A., CUIT [●], con domicilio en [●], Ciudad Autónoma de Buenos Aires. La base de datos de solicitantes y suscriptores está inscripta en el Registro Nacional de Bases de Datos de la Agencia de Acceso a la Información Pública con el N° [●], conforme al artículo 21 de la Ley N° 25.326.

Esta política abarca todos los datos que trata la aplicación habilitada "Firma Digital Argentina": los de la cuenta del usuario, los de la certificación digital y los del plan contratado. La aplicación no usa otros servidores que los de Egregor Labs en la República Argentina.

Toda información recibida por Egregor Labs, excepto la que la ley determina como pública, es confidencial y no se hace pública sin el consentimiento previo de su titular, salvo requerimiento de autoridad competente.

4. Tratamiento de la información

a) Información que se solicita

Servicio	Datos que se solicitan
Cuenta	Correo electrónico y contraseña (se guarda solo su resumen criptográfico), o el identificador que entrega Apple, Google o Microsoft cuando el usuario elige iniciar sesión con ellos, junto con el nombre y el correo electrónico que ese proveedor comparta
Certificado de persona humana — modalidad remota	CUIL o CUIT; sexo según el DNI; correo electrónico del certificado; fotografía del rostro con prueba de vida; datos técnicos del dispositivo (modelo, versión de iOS, versión de la aplicación) y atestación de la aplicación
Certificado de persona humana — modalidad presencial	Los anteriores, la exhibición del DNI y la captura de dos huellas dactilares
Certificado de persona jurídica	Los datos de la persona humana responsable, más la denominación, CUIT, cargo o función del responsable y la documentación societaria del punto 3.2.2 de la Política, que se carga en PDF desde la aplicación habilitada
Renovación	Los mismos datos que para la emisión
Portal web	Correo electrónico de la cuenta, el código de un solo uso enviado a ese correo y la dirección IP de cada ingreso
Revocación	Desde la cuenta (aplicación o portal web): la sesión, el método de inicio de sesión y la dirección IP. Por la Mesa de Ayuda: la videollamada en vivo con un Oficial de Registro (no se graba), el número de DNI leído y los controles que registra el Oficial; el Oficial consulta la foto y los datos del legajo, y cada consulta queda registrada. Presencial: los datos de esa modalidad. Por terceros: la documentación que acredite su legitimación y la causa
Plan	Plan contratado, firmas de prueba usadas, identificadores de las transacciones de la App Store (Egregor Labs no recibe datos de la tarjeta) y, para personas jurídicas, los datos de facturación
Firma de documentos	Ninguno del documento: el documento se firma en el dispositivo y no se envía a Egregor Labs. La aplicación envía solo la huella criptográfica del valor de la firma, para obtener el sello de tiempo, y el certificado usado. Egregor Labs registra la fecha, el certificado y esa huella, y descuenta la firma del plan

Servicio	Datos que se solicitan
Verificación de firmas	Del documento, solo su huella criptográfica, calculada en el dispositivo. La aplicación envía los datos de la firma (sin el contenido del documento): certificados, sello de tiempo y datos de revocación. No se guardan después de responder
Consulta de estado	Ninguno: la CRL y el servicio OCSP son de acceso libre. La consulta en el sitio web registra la dirección IP para limitar abusos
Mesa de Ayuda y reclamos	Nombre, datos de contacto y el contenido de la consulta

Del RENAPER, Egregor Labs recibe, ante un cotejo positivo, los datos de identificación del solicitante necesarios para el certificado (nombre y apellido, número de DNI, CUIL) y el resultado del cotejo.

Egregor Labs no recibe ni conoce la clave privada del suscriptor, su biometría registrada en el dispositivo ni su código de desbloqueo. La autenticación biométrica que exige cada firma se realiza íntegramente en el dispositivo; Egregor Labs no recibe datos de ella.

b) Finalidad y forma de utilización de la información

La información se utiliza exclusivamente para:

1. Validar la identidad del solicitante mediante el cotejo con el RENAPER, conforme al Decreto N° 743/2024.
2. Verificar, en su caso, la existencia de la persona jurídica y la representación invocada.
3. Verificar que la solicitud proviene de la aplicación habilitada y de un dispositivo admitido.
4. Incorporar al certificado los datos que lo integran, para vincular los datos de verificación de firma a su titular (artículo 13 de la Ley N° 25.506).
5. Emitir, notificar, renovar y revocar el certificado y comunicarse con el suscriptor sobre él.
6. Conservar la documentación de respaldo durante diez (10) años, conforme al artículo 21, inciso i) de la Ley N° 25.506.
7. Administrar la cuenta del usuario y su plan, incluido el control de las firmas de prueba.
8. Atender consultas y reclamos, y cumplir requerimientos de autoridades competentes y auditorías.

La información no se usa para ningún fin ajeno a la Política. Egregor Labs no envía publicidad al suscriptor por intermedio del servicio de certificación sin su consentimiento expreso (artículo 21, inciso 12 del Anexo al Decreto N° 182/2019). Los datos biométricos (fotografía del rostro y huellas) se tratan con las medidas propias de los datos sensibles, se usan solo para la validación de identidad y no se usan para ninguna otra finalidad.

c) Información contenida en el certificado y su publicación

El certificado contiene los datos del punto 3.1.2 de la Política:

- **Persona humana:** nombre y apellido según el DNI; CUIL o CUIT; país; y correo electrónico.
- **Persona jurídica:** denominación; CUIT; unidad operativa (si corresponde); país; y nombre, CUIL o CUIT y cargo de la persona responsable de la custodia de la clave.

Los datos contenidos en un certificado son de carácter público: viajan con cada documento firmado y Egregor Labs está obligada a permitir la consulta de los certificados emitidos y de su estado. La consulta en el sitio web requiere el número de serie o el CUIL o CUIT exacto; Egregor Labs no publica listados masivos de certificados emitidos. La información sobre la revocación de un certificado no es confidencial y se publica en la CRL y en el servicio OCSP.

d) Información adicional opcionalmente remitida

Si el solicitante o suscriptor remite información adicional a la requerida, Egregor Labs la trata como confidencial, la conserva en el legajo identificada como no verificada (artículo 14, inciso b), apartado 3 de la Ley N° 25.506), no la incluye en el certificado y no la usa para otro fin que el que motivó su envío.

e) Consecuencias de proporcionar los datos, de negarse o de su inexactitud

Los datos solicitados son necesarios para emitir el certificado. Si el solicitante se niega a proporcionarlos o a prestar su consentimiento para el cotejo con el RENAPER, no puede emitirse el certificado. La inexactitud de los datos impide la validación, provoca el rechazo de la solicitud o, si se detecta después, la revocación del certificado (punto 4.9.1 de la Política), y puede generar responsabilidad para quien los proporcionó.

f) Derechos de acceso, rectificación, actualización y supresión

El titular de los datos, previa acreditación de su identidad, puede ejercer en forma gratuita los derechos de acceso, rectificación, actualización y supresión de sus datos personales (artículos 14, 15 y 16 de la Ley N° 25.326), escribiendo a privacidad@firmadigitalapp.com.ar o desde la aplicación habilitada. El acceso se responde dentro de los diez (10) días corridos, y la rectificación, actualización o supresión dentro de los cinco (5) días hábiles.

Eliminación de la cuenta. El usuario puede eliminar su cuenta en cualquier momento desde la aplicación habilitada (Perfil) o desde el portal web https://firmadigitalapp.com.ar/cuenta, escribiendo la frase “eliminar mi cuenta”. La eliminación es inmediata: se revocan todos los certificados vigentes del suscriptor, se cancelan los trámites en curso y se borran los datos de acceso (correo electrónico, resumen de la contraseña y vínculos con Apple, Google o Microsoft, incluida la revocación de la autorización otorgada a Apple), las sesiones abiertas y, en el dispositivo, las claves y los certificados. Egregor Labs confirma la eliminación por correo electrónico. Las suscripciones de la App Store las administra Apple y se cancelan desde la configuración del dispositivo.

La rectificación de un dato incluido en un certificado implica su revocación y, si se solicita, la emisión de uno nuevo. La supresión no procede respecto de la documentación de respaldo que Egregor Labs debe conservar por diez (10) años según el artículo 21, inciso i) de la Ley N° 25.506, ni respecto de los datos de certificados ya emitidos y de su estado, cuya publicación es obligatoria.

La Agencia de Acceso a la Información Pública, en su carácter de órgano de control de la Ley N° 25.326, tiene la atribución de atender las denuncias y reclamos que se interpongan por incumplimiento de las normas sobre protección de datos personales.

g) Medidas técnicas y organizativas de seguridad y confidencialidad

Conforme al artículo 9 de la Ley N° 25.326, Egregor Labs adopta medidas para evitar la adulteración, pérdida, consulta o tratamiento no autorizado de los datos, y para detectar desviaciones de información intencionales o no, provengan de la acción humana o del medio técnico. Entre otras:

- **Ubicación y aislamiento.** Los datos se tratan y almacenan en la infraestructura tecnológica de Egregor Labs, situada en la República Argentina, con los niveles de seguridad física del Plan de Seguridad y separada de los servicios de la aplicación que no forman parte de la certificación.
- **Cifrado.** La aplicación habilitada transmite los datos a la Autoridad de Registro cifrados con TLS. Los legajos se almacenan cifrados con claves gestionadas en un módulo de seguridad de hardware (HSM).
- **Minimización en el dispositivo.** La aplicación no guarda en el dispositivo la fotografía del rostro ni la documentación enviada. Los documentos que el usuario firma o verifica no salen del dispositivo.
- **Portal web.** Se ingresa con un código de un solo uso enviado al correo de la cuenta; la sesión dura treinta (30) minutos y la respuesta al pedido de código no revela si un correo tiene cuenta.
- **Control de acceso.** Solo el personal con roles de confianza que lo necesita para su función accede a los datos, con cuentas nominativas, ingreso con passkey (con biometría o llave de seguridad, sin contraseñas) y registro de cada acceso y de cada consulta de documentación o de la foto del legajo.
- **Personal.** Todo el personal firma un acuerdo de confidencialidad, recibe capacitación en protección de datos y está sujeto al régimen de sanciones del Manual de Procedimientos.
- **Registro y monitoreo.** Los accesos y operaciones quedan registrados en registros protegidos contra modificación y se revisan periódicamente.
- **Respaldo.** Copias cifradas en el sitio de contingencia, también en el país.
- **Evaluaciones.** Auditorías internas y externas, y pruebas de seguridad periódicas de la infraestructura y de la aplicación habilitada.

h) Cesión de los datos

Los datos recabados para emitir el certificado no son objeto de cesión, salvo las excepciones del artículo 11 de la Ley N° 25.326 (entre ellas, el requerimiento judicial o de autoridad

administrativa competente). La consulta al RENAPER para validar la identidad no constituye una cesión: se realiza en el marco del convenio de confronte de datos, con el consentimiento del titular y solo para verificar su identidad. Los datos públicos del certificado se publican según el punto c).

Egregor Labs no transfiere fuera del país los datos de identidad, las capturas biométricas ni la documentación de los solicitantes. Cuando el usuario elige iniciar sesión con Apple, Google o Microsoft, ese proveedor, fuera del país, conoce que usa Egregor Labs y comparte con Egregor Labs su identificador, su nombre y su correo electrónico; y cuando contrata un plan desde la aplicación, Apple procesa el pago fuera del país. Esos tratamientos se rigen por las políticas de cada proveedor y se realizan con el consentimiento del usuario (artículo 12 de la Ley N° 25.326). Las notificaciones de la aplicación se envían a través del servicio de Apple sin datos personales en su contenido. Los proveedores que prestan servicios de infraestructura tecnológica a Egregor Labs acceden a los datos solo en la medida necesaria para prestar el servicio, bajo obligación de confidencialidad y conforme al artículo 25 de la Ley N° 25.326.

i) Contacto

Los titulares de los datos y los terceros usuarios pueden ejercer sus derechos, formular consultas o realizar comentarios y sugerencias en:

Responsable de protección de datos	[Nombre]
Correo electrónico	privacidad@firmadigitalapp.com.ar
Teléfono	[●]
Domicilio	[●], Ciudad Autónoma de Buenos Aires

j) Secreto profesional

Egregor Labs, como responsable de la base de datos, y todas las personas que intervienen en cualquier fase del tratamiento están obligadas a guardar el secreto profesional sobre los datos personales, obligación que subsiste aun después de finalizada su relación con el suscriptor o con Egregor Labs. Egregor Labs solo puede ser relevada del deber de secreto por resolución judicial o de autoridad administrativa competente, o cuando medien razones fundadas relativas a la seguridad pública, la defensa nacional o la salud pública (artículo 10 de la Ley N° 25.326).

5. Plazo de conservación

Datos	Plazo
Legajo de emisión, renovación y revocación (incluidas capturas biométricas y resultados del RENAPER)	Diez (10) años desde la expiración o revocación del certificado
Solicitudes no completadas o rechazadas	Diez (10) años desde el rechazo, como información relativa a una solicitud
Certificados emitidos y CRL	Diez (10) años desde su expiración

Datos	Plazo
Consultas de la Mesa de Ayuda	Dos (2) años, salvo que se vinculen a un reclamo
Datos de acceso de la cuenta (correo, contraseña, vínculos con Apple, Google o Microsoft, sesiones)	Hasta que el usuario elimina su cuenta: se borran en ese momento
Datos del plan	El registro del plan por CUIL (incluidas las firmas de prueba usadas, para que la prueba no se otorgue dos veces) y los registros de pago que exija la normativa fiscal, por los plazos legales
Registro de firmas (fecha, certificado y huella de la firma, nunca el documento)	Diez (10) años, como registro de uso del certificado
Datos enviados para verificar una firma	No se conservan

Cumplido el plazo, los datos se destruyen en forma segura y con registro.

6. Modificaciones

Las modificaciones de esta política requieren la aprobación previa del Ente Licenciante, se publican en el sitio web y se notifican a los suscriptores con certificados vigentes en la aplicación habilitada y por correo electrónico.