

Política de Seguridad de la Información

Lexiware SAS — CUIT 30-71962959-4 — plataforma Firmana (www.firmana.app)

Base de datos inscripta en la AAIP: EX-2026-99411305- -APN-DNPDP#AAIP

Ejercicio de derechos sobre datos personales: acceso@lexiware.com.ar

Versión 1.2 — 01/10/2026

1. Objeto y alcance

Esta política establece las medidas con que Lexiware SAS protege la confidencialidad, integridad y disponibilidad de la información que trata en Firmana, su plataforma de firma electrónica y digital de documentos. Alcanza a los datos de las organizaciones clientes y sus usuarios, a los documentos que se firman, a los datos de las personas firmantes y, en particular, a los datos de verificación de identidad (número y datos del DNI, imágenes del documento, selfies y resultados de las validaciones).

2. Marco normativo

Ley 25.326 de Protección de los Datos Personales y su reglamentación; disposiciones y resoluciones de la Agencia de Acceso a la Información Pública sobre medidas de seguridad; Ley 25.506 de Firma Digital. Las bases de datos personales se inscriben en el Registro Nacional de Bases de Datos.

3. Roles y responsabilidades

- **Responsable legal de Lexiware SAS:** aprueba esta política, responde las solicitudes de los titulares de los datos y decide sobre el tratamiento.
- **Responsable técnico / administrador de sistemas:** administra la infraestructura, los respaldos y la seguridad, y gestiona los incidentes. Es la única función con acceso administrativo a la base de datos.
- **Operador de la plataforma:** gestiona los planes y cupos de las organizaciones clientes.
- **Usuarios de las organizaciones clientes:** acceden sólo a los datos de su propia organización según su rol (Administrador, Emisor o Consulta). Sólo Administradores y Emisores ven las imágenes de identidad de los documentos que gestionan.
- **Personas firmantes:** acceden únicamente a su propio documento, mediante un enlace personal.

4. Clasificación de la información

Los datos de verificación de identidad se tratan como información de máxima sensibilidad: se guardan cifrados, con acceso restringido y registrado, y nunca se incorporan al PDF firmado, a los correos electrónicos ni a las respuestas de la interfaz de programación (API). Los documentos y datos de contacto se tratan como información confidencial de cada organización cliente.

5. Control de acceso

- Acceso por usuario y contraseña personal; contraseñas almacenadas con Argon2id. Inicio de sesión con Google disponible.
- Roles y permisos por organización, con aislamiento entre organizaciones.
- Límite de intentos de inicio de sesión y posibilidad de cerrar todas las sesiones de un usuario.
- Las claves de API se guardan sólo como huella SHA-256, tienen alcance de lectura o escritura y se pueden revocar.
- Los enlaces de firma y los códigos de verificación se guardan sólo como huella SHA-256 y nunca se registran en los logs.
- Cada visualización de una imagen de identidad queda registrada en el registro de auditoría, con usuario y fecha.

6. Criptografía

- Todo el tráfico viaja cifrado con TLS (HTTPS obligatorio).
- Las imágenes de identidad se cifran en reposo con AES-256-GCM.
- Los documentos firmados llevan firma digital PAdES y sellos de tiempo RFC 3161.
- Las claves y secretos se administran como secretos de la infraestructura, fuera del código. La clave raíz de la autoridad de certificación propia se conserva fuera de línea.

7. Seguridad de la infraestructura

- La plataforma se aloja en la nube de Fly.io (región São Paulo). La seguridad física de los centros de datos (control de acceso, videovigilancia y seguridad perimetral) está a cargo del proveedor.
- Sólo se expone a Internet el acceso web por HTTPS. La base de datos no tiene acceso público: se comunica por la red privada cifrada del proveedor, y el acceso administrativo requiere credenciales y un túnel autenticado.
- Los servicios internos (lectura de documentos, verificación facial, firma digital) se comunican con la aplicación por la red privada.
- La interfaz de programación aplica límites de uso por clave.
- Se usan componentes de código abierto con licencias verificadas, y se actualizan.

8. Integridad y trazabilidad

- Cada documento tiene su huella SHA-256 y cada paso de la firma se registra en una cadena de eventos enlazados por hash.
- Los eventos clave (consentimiento y firma) reciben un sello de tiempo de un tercero (RFC 3161).
- El paquete probatorio de cada documento se ancla en blockchains públicas (Bitcoin, mediante OpenTimestamps, y Polygon), lo que permite detectar cualquier alteración posterior.
- Se mantiene un registro de auditoría de las acciones relevantes de los usuarios y del sistema.

9. Minimización, finalidad y conservación

Sólo se recolectan los datos necesarios para la firma y la verificación de identidad que el emisor eligió. Los datos se usan exclusivamente para esa finalidad, y no se ceden a terceros salvo obligación legal. Se conservan por el tiempo necesario para la finalidad y las obligaciones legales; los titulares pueden ejercer sus derechos de acceso, rectificación y supresión en los plazos de la Ley 25.326.

10. Uso del Sistema de Identidad Digital (SID) del RENAPER

- La consulta se realiza una vez por firmante y por documento, en el momento de la firma y con el consentimiento expreso de la persona.
- Los resultados se usan sólo para verificar la identidad de esa firma y constan en la constancia de la firma; no se usan con otra finalidad ni se ceden.
- Cada consulta queda registrada (persona, documento, fecha y resultado) en el registro de auditoría.
- Las credenciales de acceso al servicio se guardan como secretos de la infraestructura y sólo las usa el servicio interno de verificación.

11. Respaldo y continuidad

La base de datos tiene copias de seguridad automáticas diarias, con retención de 30 días, y además se generan respaldos completos verificados. Los procedimientos de restauración están documentados.

12. Gestión de incidentes

Ante un incidente de seguridad, el responsable técnico lo contiene, lo registra y analiza su causa y alcance. Si afecta datos personales, se informa al responsable legal, a las organizaciones afectadas y, cuando corresponda, a la autoridad de control y a los titulares de los datos, y se adoptan medidas para evitar que se repita.

13. Proveedores

Se eligen proveedores de infraestructura con controles de seguridad reconocidos, y se limita a cada uno la información estrictamente necesaria para prestar su servicio.

14. Revisión

Esta política se revisa al menos una vez por año y ante cambios relevantes de la plataforma o de la normativa.

Aprobada por: _____

Representante legal de Lexiware SAS

Fecha: 01/10/2026