LITIGIAR

Seguridad, Confidencialidad y Cumplimiento Normativo

Documento técnico-jurídico · Argentina Litigia (LitigiAR)

Ley 25.326 | Ley 26.388 | Ley 23.187 | Convenio Budapest | AES-256-GCM | 100% gratuito

Última actualización: 24 de abril de 2026 · Versión 2.0 · Documento supervisado por profesional del derecho

Servicio 100% gratuito

Actualmente **LitigiAR se ofrece sin costo alguno**. No se cobran suscripciones, no existe plan arancelado activo y no se procesan pagos. Si en el futuro se habilitaran funciones pagas, se actualizará el presente documento y se requerirá consentimiento expreso del usuario conforme `art. 5 Ley 25.326` .

Síntesis ejecutiva

LitigiAR no transmite a servidores externos el contenido de los expedientes judiciales, notas del profesional, datos del cliente ni documentación amparada por el secreto profesional `art. 7 inc. c Ley 23.187` . El procesamiento del expediente se realiza localmente en el dispositivo del usuario, dentro de los portales oficiales (MEV SCBA, Portal PJN) donde éste ya se encuentra autenticado. El único tráfico hacia la infraestructura del responsable se limita a autenticación de cuenta, verificación del estado del servicio (actualmente gratuito) y comunicaciones transaccionales. Todo este comportamiento es verificable técnicamente por el propio usuario (Secciones 5 y 6).

ÍNDICE

15. Obligaciones del usuario e indemnidad
16. Ley aplicable y jurisdicción
17. Contacto del responsable

1. Responsable del tratamiento de datos

Identificación conforme art. 6 Ley 25.326

- **Nombre comercial:** LitigiAR
- **Responsable / Titular:** Argentina Litigia
- **Dominio:** argentinalitigia.com
- **Domicilio electrónico para notificaciones:** privacidad@argentinalitigia.com
- **ID oficial Chrome Web Store:** `gfindnmlofncoplclckgicpdchfbhgla`
- **Jurisdicción del responsable:** La Plata, Provincia de Buenos Aires, República Argentina
- **Departamento Judicial:** La Plata (SCBA)

2. Marco normativo aplicable

El servicio se sujeta a las siguientes normas vigentes en la República Argentina:

Norma	Alcance aplicado
Ley 25.326 Protección de Datos Personales	Régimen general del tratamiento de datos. Derechos ARCO, consentimiento, principios de licitud, finalidad y calidad. Autoridad de aplicación: AAIP.
Dto. 1558/2001 Reglamentación Ley 25.326	Reglamento de seguridad, consentimiento, transferencias y derechos.
Res. AAIP 47/2018 Medidas de seguridad recomendadas	Clasificación de niveles de seguridad (básico, medio, crítico). El tratamiento realizado por LitigiAR encuadra en nivel **medio** (datos profesionales, matrícula, documentos de identidad).
Ley 26.388 Delitos informáticos	Tipificación de acceso indebido (art. 153 bis CP), violación de secretos informáticos (art. 157 bis CP), daño informático (art. 183 CP), entre otros.
Ley 27.411 Convenio de Budapest sobre Ciberdelincuencia	Argentina ratificó el Convenio del Consejo de Europa sobre cooperación internacional en ciberdelitos.
Ley 5.177 (PBA) Ejercicio de la Abogacía	Jurisdicción primaria del responsable. Secreto profesional del abogado en territorio bonaerense (arts. 58 inc. 7 y concordantes). Sanciones disciplinarias del Colegio de Abogados del Departamento Judicial correspondiente.
Ley 23.187 (CABA) Ejercicio de la Abogacía	Aplicable supletoriamente a los usuarios profesionales matriculados en CABA. Secreto profesional (art. 6 inc. f y art. 7 inc. c).
Código Penal	Arts. 153, 153 bis, 155, 156, 157 bis, 183 y 197 CP — tipificación de conductas

	contra la privacidad y seguridad informática.
Código Civil y Comercial	Arts. 52, 53 (derecho a la intimidad y a la imagen); arts. 1716-1780 (responsabilidad civil).
Ley 24.240 Defensa del Consumidor	Aplicable con las limitaciones propias de un servicio gratuito (arts. 1 y 2). Se respetan deberes de información y no discriminación.
Ley 25.506 Firma Digital	Aplicable a la integración opcional con sistemas de firma digital AFIP.
Ley 11.723 Propiedad Intelectual	Protege el software propio de LitigiAR y el contenido generado por el usuario.

3. Datos tratados: qué viaja y qué no

La arquitectura del servicio implementa el principio de **minimización** del `art. 4 inc. 1 Ley 25.326` : sólo se tratan los datos estrictamente necesarios para la prestación del servicio, sin exceso ni duplicación.

SÍ SE TRANSMITEN AL SERVIDOR (MÍNIMO TÉCNICO)

- **Credenciales de cuenta del servicio** — email y contraseña en el login; contraseña hasheada con `bcrypt` (10 rounds) server-side. Nunca se almacena la contraseña en texto plano.
- **Token JSON Web Token (JWT)** — firmado con clave secreta server-side; permite mantener sesión sin reenviar credenciales.
- **Verificación de estado del servicio** — consulta periódica al endpoint `/auth/plan` (cacheado 60 segundos). Actualmente el estado es "gratuito" para todos los usuarios.
- **Datos del perfil profesional voluntariamente cargados** — nombre, apellido, matrícula, tomo/folio, universidad. Destinados a personalizar encabezados de escritos generados por el usuario.
- **Eventos de uso anonimizados** — ej: `abrio_calculadora_laboral` , sin contenido. Finalidad: estadística operativa y detección de errores (`art. 4 inc. 2 Ley 25.326`).

NUNCA SE TRANSMITEN AL SERVIDOR

- **Contenido de expedientes judiciales**: carátulas, partes, providencias, resoluciones, sentencias.
- **Datos personales de clientes, contrapartes, testigos o terceros** mencionados en los expedientes.
- **Notas profesionales del abogado**, estrategia procesal, memorandos internos.
- **Cálculos de plazos, liquidaciones, honorarios e intereses** realizados por el usuario.
- **Escritos redactados** con las plantillas.
- **Causas seguidas** en el módulo Watchdog.
- **Credenciales de MEV SCBA, PJN y otros portales judiciales** — cifradas localmente con AES-256-GCM.
- **Información amparada por el secreto profesional** `art. 7 inc. c Ley 23.187` / `art. 58 Ley 5.177 PBA` .

Todo dato no transmitido se almacena exclusivamente en `chrome.storage.local` , estructura de almacenamiento nativa del navegador del usuario, bajo el control exclusivo de éste. Al desinstalar la extensión, Chrome elimina automáticamente dichos datos del dispositivo.

4. Permisos técnicos de la extensión

Los permisos declarados en el archivo `manifest.json` son públicamente auditables desde el propio listado del Chrome Web Store. Cada permiso responde al principio de **necesidad operativa**:

Permiso	Finalidad y fundamento
`storage`	Almacenamiento local de configuración, causas seguidas, notas y credenciales cifradas. Los datos no son accesibles por otros sitios web ni extensiones.
`alarms`	Tareas en segundo plano (chequeo periódico de causas, recordatorios de plazos). Todas las tareas corren en el dispositivo del usuario.
`tabs`	Detección del dominio actualmente activo para determinar si corresponde activar el panel (únicamente en MEV SCBA y Portal PJN).
`notifications`	Emisión de alertas locales sobre plazos próximos a vencer (API nativa de Chrome Notifications, no se transmite nada externamente).
`clipboardWrite`	Botones "copiar al portapapeles" para encabezados, cálculos y escritos.
`identity`	Autenticación mediante Google OAuth 2.0 (opcional). Alternativa: email y contraseña tradicionales.
`debugger`	Reservado para integración con firma digital AFIP (token/dispositivo criptográfico). Funcionalidad no activada por defecto; el usuario debe habilitarla voluntariamente.
`downloads`	Descarga de PDFs generados localmente (informes, escritos, liquidaciones).

5. Dominios autorizados de comunicación

El archivo `manifest.json` declara la lista cerrada de dominios (`host_permissions`) a los que la extensión puede conectarse. **El propio navegador Chrome impide, a nivel de su motor de ejecución, cualquier intento de conexión a dominios no listados**. Se trata de una restricción enforced por el propio browser, independiente del código de la extensión.

Dominio	Finalidad	¿Transmite datos del expediente?
`*.scba.gov.ar`	Portal oficial SCBA donde el usuario se encuentra trabajando.	**NO** — únicamente lectura local del DOM.
`mev.pjn.gov.ar` `eje.pjn.gov.ar`	Portal oficial del Poder Judicial de la Nación.	**NO** — lectura local.
`argentinalitigia.com`	Autenticación, verificación de estado del servicio, comunicaciones transaccionales.	**SÍ** (únicamente los datos enumerados en Sección 3, columna izquierda).
`apis.datos.gob.ar`	Datos públicos INDEC (IPC, UVA, CER, canasta básica).	**NO** — sólo consulta pública.

`raw.githubusercontent.com`	Valores oficiales auto-actualizados (JUS, bono colegio, tasas BCRA).	**NO** — sólo descarga.

`saij.gob.ar`
`infoleg.gob.ar`
`boletinoficial.gob.ar`
	Buscador jurídico integrado (fallos, leyes, normativa).	**NO** — consulta pública a bases de datos oficiales.

`colproba.org.ar`	Cotización oficial del bono Colegio de Abogados PBA.	**NO**.

6. Verificación técnica del tráfico por el propio usuario

El usuario puede auditar **en tiempo real** todo el tráfico de red generado por LitigiAR utilizando las herramientas integradas en Chrome, sin necesidad de instalar software adicional. Procedimiento:

1

Acceder al portal oficial donde se utilizará la extensión

Ingresar normalmente a mev.scba.gov.ar o al portal correspondiente. La extensión se activa automáticamente tras la carga del DOM.

2

Abrir las herramientas de desarrollador del navegador

Tecla F12 o clic derecho sobre la página → "Inspeccionar". Se despliega el panel DevTools.

3

Seleccionar la pestaña "Network"

En DevTools, pestaña "Network" (Red). Esta vista registra la totalidad de las peticiones de red que realiza el navegador desde la apertura de las herramientas.

4

Aplicar el filtro "Fetch/XHR"

Permite visualizar exclusivamente las comunicaciones programáticas (AJAX), excluyendo recursos estáticos (CSS, imágenes).

5

Operar LitigiAR con normalidad

Ejecutar las funciones de la extensión: abrir expedientes, calcular plazos, generar escritos, consultar histórico.

6

Examinar el listado de peticiones

Las únicas conexiones de red registradas corresponderán a los dominios declarados en la Sección 5. **Cualquier conexión a un dominio no autorizado constituiría un incidente de seguridad** y debería notificarse conforme Sección 13.

7

Inspeccionar el contenido de cada petición

Seleccionando una petición individual, pestaña Payload / Request, puede examinarse el cuerpo exacto del requerimiento, verificando que no contenga datos del expediente.

7. Arquitectura de seguridad: 5 capas superpuestas

Conforme al principio de **defensa en profundidad** recomendado por la Res. AAIP 47/2018, LitigiAR implementa cinco mecanismos independientes de protección:

1 **Sandboxing del navegador**

Chrome bloquea a nivel del motor de ejecución cualquier conexión a dominios no declarados en `host_permissions`. No depende del código propio de la extensión.

2 **Código fuente auditable**

Las extensiones Chrome no se distribuyen minificadas ni ofuscadas. Mediante herramientas de auditoría públicas (CRXviewer, CRXcavator) cualquier profesional puede analizar el código completo de LitigiAR.

3 **Revisión previa de Google**

El proceso de publicación en el Chrome Web Store exige revisión técnica y de políticas. LitigiAR cuenta con ID oficial `gfindnmlofncoplclckgicpdchfbhgla`.

4 **Cifrado en tránsito y en reposo**

Todas las comunicaciones server-side utilizan TLS 1.2 o superior. Las credenciales de portales judiciales se almacenan localmente cifradas con AES-256-GCM. Las contraseñas de cuenta se hashan con bcrypt.

5 **Principio de minimización**

Solamente se recopilan los datos imprescindibles (`art. 4 inc. 1 Ley 25.326`). El contenido del expediente nunca abandona el dispositivo del usuario.

8. Medidas técnicas de seguridad

Clasificación según Res. AAIP 47/2018

Los datos tratados por LitigiAR se clasifican en **nivel medio** (datos identificatorios, profesionales y documentos de identidad). Se implementan las medidas correspondientes a dicho nivel:

8.1 Credenciales de portales judiciales (si el usuario decide guardarlas)

```
Algoritmo:    AES-256-GCM (estándar NIST SP 800-38D)
Longitud:     256 bits
Vector IV:    12 bytes aleatorios por cada operación
Auth tag:     16 bytes (GCM mode)
Storage:      chrome.storage.local (dispositivo del usuario)
Aislamiento:  Sandbox del navegador — ninguna otra extensión o sitio
              puede acceder al almacén de LitigiAR
Persistencia: Se elimina automáticamente al desinstalar la extensión
```

8.2 Contraseñas server-side (cuenta LitigiAR)

```
Algoritmo:    bcrypt
Rounds:       10 (cost factor)
Salt:         16 bytes aleatorios, único por usuario
Storage:      No se almacena la contraseña en texto plano en ningún momento.
```

8.3 Documentos cargados al marketplace profesional

```
Finalidad:    Verificación de identidad y matrícula profesional
Cifrado:      AES-256-GCM antes de persistir a disco
Ubicación:    Fuera del webroot, directorio /data/marketplace-docs/
Permisos:     0600 (acceso exclusivo del proceso server)
Acceso:       Sólo el administrador autenticado, con audit log
              persistente de cada visualización (quién, cuándo, IP)
Retención:    Máximo 90 días post-verificación
Destrucción:  Se conserva únicamente el hash SHA-256 del documento
              original como prueba criptográfica de autenticidad
```

9. Secreto profesional del abogado usuario

LitigiAR ha sido diseñado reconociendo que el usuario — **el abogado matriculado** — se encuentra obligado al deber de secreto profesional tipificado en:

- **Art. 58 Ley 5.177 PBA** (ejercicio en Provincia de Buenos Aires): deber de guardar "rigurosamente el secreto profesional" sobre los asuntos que se le hubieren confiado.
- **Art. 7 inc. c Ley 23.187** (ejercicio en CABA): obligación análoga para matriculados en la Ciudad Autónoma de Buenos Aires.
- **Art. 156 Código Penal**: al que teniendo noticia de un secreto por razón de su estado, oficio, empleo, profesión o arte, lo revelare sin justa causa, se le impone **multa e inhabilitación especial de seis (6) meses a tres (3) años**.
- **Sanciones disciplinarias**: infracción del deber de secreto puede derivar en sanciones del Colegio de

Abogados correspondiente al Departamento Judicial de matrícula (apercibimiento, suspensión o cancelación de la matrícula).

La decisión arquitectónica de **no transmitir el contenido del expediente a servidores externos** responde precisamente al objetivo de no comprometer el cumplimiento del deber profesional del usuario. Una herramienta que expusiera información amparada por secreto profesional convertiría al profesional en potencial infractor penal y disciplinario.

10. Marco de responsabilidades penales en materia informática

La Ley 26.388 incorporó al Código Penal argentino diversos tipos penales relativos a la información electrónica. LitigiAR opera respetando estrictamente dichos tipos y aclara su posición respecto a cada uno:

Tipo penal	Conducta del responsable
Art. 153 CP — apertura, acceso o interceptación indebida de comunicaciones electrónicas	El servicio no intercepta comunicaciones. El usuario accede voluntariamente a los portales judiciales mediante sus propias credenciales.
Art. 153 bis CP — acceso indebido a sistema informático	LitigiAR no accede a ningún sistema al que el usuario no tenga previamente autorización. Únicamente opera sobre el DOM ya cargado por el navegador.
Art. 155 CP — publicación indebida de correspondencia electrónica	No se accede ni publica correspondencia del usuario.
Art. 157 bis CP — violación de secretos y bases de datos personales	No se insertan, alteran ni exfiltran datos personales de bases ajenas. La base de datos propia se protege conforme Res. AAIP 47/2018.
Art. 183 CP — daño informático	La extensión no modifica, borra ni inutiliza datos de terceros. Todos los cambios al DOM son visuales (panel lateral).
Art. 197 CP — interrupción de comunicaciones	La extensión no interrumpe ni altera canales de comunicación.

11. Derechos del titular (ARCO)

Conforme `arts. 14, 15, 16 y 17 Ley 25.326`, el titular de los datos goza de los siguientes derechos, ejercitables sin costo:

- **Acceso** (art. 14): conocer qué datos personales son tratados y con qué finalidad.
- **Rectificación** (art. 16): corregir datos inexactos o incompletos.
- **Cancelación / Supresión** (art. 16): eliminar los datos cuando ya no sean necesarios o cuando así lo requiera el titular.
- **Oposición** (art. 27 Dto. 1558/2001): oponerse a determinados tratamientos.

Para ejercer cualquiera de estos derechos, enviar solicitud a **privacidad@argentinalitigia.com** con asunto "`DERECHOS ARCO`", indicando nombre completo, DNI, email registrado y derecho que se solicita ejercer. Plazo de respuesta: **10 días corridos** (acceso) / **5 días** (rectificación o supresión), conforme reglamentación.

Ante la falta de respuesta o insatisfacción, el titular puede interponer denuncia ante la **Agencia de Acceso a la Información Pública (AAIP)**, autoridad de aplicación: argentina.gob.ar/aaip.

12. Retención y supresión de datos

Categoría de dato	Plazo de retención
Credenciales de cuenta (email, hash de contraseña)	Mientras exista la cuenta activa. Supresión a solicitud del titular.
Datos del perfil profesional	Mientras la cuenta esté activa.
Documentos del marketplace (DNI, matrícula, facturas)	Máximo 90 días post-verificación. Se conserva únicamente hash SHA-256.
Logs técnicos del servidor	Hasta 30 días para detección de errores, luego supresión automática.
Eventos de analítica anonimizada	Hasta 12 meses, agregados sin identificación del usuario.
Datos almacenados localmente (chrome.storage.local)	Bajo control exclusivo del usuario. Se eliminan automáticamente al desinstalar la extensión.

13. Notificación de vulnerabilidades e incidentes

Procedimiento de disclosure responsable

Cualquier persona que detecte una vulnerabilidad, exposición de datos o conducta sospechosa puede notificarlo enviando un correo a **privacidad@argentinalitigia.com** con asunto `[SECURITY]`. El responsable se compromete a:

- Acusar recibo en **48 horas hábiles**.
- Analizar el reporte y responder con diagnóstico preliminar en **7 días corridos**.
- Publicar el fix en los plazos razonables según la severidad.
- Reconocer públicamente al reportante (si así lo desea).

Se solicita **no divulgar públicamente** la vulnerabilidad antes de la publicación del fix (disclosure responsable).

Notificación obligatoria de incidentes

En caso de brecha de seguridad que afecte datos personales, el responsable se obliga a:

- Notificar a los titulares afectados por email, dentro de las **72 horas** de conocido el incidente.
- Informar a la AAIP conforme `Resolución 47/2018`, cuando corresponda por severidad.
- Publicar un informe post-mortem con causa raíz y medidas correctivas.

14. Naturaleza jurídica y responsabilidad contractual

14.1 Naturaleza jurídica del vínculo

La instalación y utilización de LitigiAR, sumada a la registración de una cuenta y la aceptación de los presentes términos, configura una **relación contractual gratuita** entre el responsable y el usuario. El carácter gratuito del servicio **no excluye la aplicación de la Ley 24.240 de Defensa del Consumidor** cuando el vínculo encuadre como relación de consumo (`art. 1 Ley 24.240` y `art. 1093 CCyCN`), según lo tiene dicho la jurisprudencia (Fallos CSJN "Rodríguez, María Belén c/ Google" y concordantes).

En consecuencia, son aplicables al presente vínculo las normas sobre contratos, la Ley 25.326, la Ley 24.240, y el régimen general de responsabilidad civil del Código Civil y Comercial (Libro Tercero, Título V).

14.2 Obligación de medios — no de resultado

La prestación del servicio constituye una **obligación de medios** (`art. 1768 CCyCN` y concordantes): el responsable se obliga a desplegar la diligencia profesional exigible al sector (`art. 1725 CCyCN`) y a implementar las medidas técnicas razonablemente disponibles al estado del arte, pero **no garantiza resultados específicos** tales como la exactitud absoluta de cálculos, clasificaciones normativas, plazos procesales, sugerencias o cualquier otro output generado por la herramienta.

En particular, las calculadoras, clasificaciones de movimientos, plazos, citas de jurisprudencia y resultados de la herramienta revisten carácter **orientativo**. El usuario profesional es quien decide, bajo su propio criterio y responsabilidad, incorporar o no dichos resultados a sus presentaciones judiciales, debiendo verificarlos previamente contra las fuentes oficiales vigentes.

14.3 Factor de atribución

La responsabilidad del responsable frente al usuario se rige por:

- **Factor subjetivo** (`arts. 1724 y 1725 CCyCN`) en cuanto al funcionamiento de la herramienta, la exactitud de cálculos y la prestación del servicio en general. Requiere acreditar culpa o dolo del responsable.
- **Factor objetivo** (`arts. 1757 y 1758 CCyCN`) en cuanto al deber de guarda y seguridad de los datos personales tratados, conforme el riesgo propio de la actividad de tratamiento.

Respecto del factor objetivo, el responsable se exonera acreditando la **causa ajena**: hecho del damnificado (`art. 1729 CCyCN`), caso fortuito o fuerza mayor (`art. 1730 CCyCN`) o hecho de un tercero por el cual no se debe responder (`art. 1731 CCyCN`).

14.4 Supuestos de exoneración

Sin perjuicio de los factores de atribución, el responsable queda exonerado de responsabilidad en los siguientes supuestos enunciativos:

- **Caso fortuito o fuerza mayor**: ataques informáticos de sofisticación no neutralizable con las medidas

de seguridad estándar del sector al momento del hecho, incluyendo ataques de día cero, DDoS masivos, o cortes generalizados de infraestructura de terceros (cloud, CDN, proveedores ISP).

- **Hecho del damnificado**: uso del servicio en contravención a estos términos; divulgación negligente de credenciales por el propio usuario; instalación de software malicioso en el dispositivo del usuario; uso de la herramienta para finalidades ilícitas.
- **Hecho de un tercero**: conductas ilícitas de terceros no vinculados al responsable (proveedores de servicios hackeados, sistemas judiciales externos, empleados del propio estudio del usuario, etc.).
- **Modificaciones normativas posteriores**: cambios en la legislación, jurisprudencia o acordadas judiciales que el sistema aún no hubiere incorporado al momento del hecho.
- **Caídas o modificaciones de portales oficiales**: indisponibilidad de MEV SCBA, Portal PJN, SAIJ, Infoleg o cualquier sistema estatal externo.
- **Uso profesional incorrecto**: errores de interpretación, de imputación al expediente, de aplicación al caso concreto u otros derivados del criterio del usuario profesional, quien por su matrícula cuenta con la idoneidad para evaluar los resultados.

14.5 Límite cuantitativo de responsabilidad

Sin perjuicio de los supuestos de exoneración, en aquellos casos en que se declarare judicialmente la responsabilidad del responsable por daños derivados del uso del servicio, el monto indemnizatorio queda **limitado a la suma equivalente a diez (10) JUS del Colegio de Abogados de la Provincia de Buenos Aires** vigentes al momento del hecho, por usuario y por evento.

Esta limitación cuantitativa **no es oponible** en los siguientes supuestos:

- Dolo del responsable o de las personas por quienes debe responder (`art. 1743 CCyCN`).
- Cláusulas declaradas abusivas conforme `art. 37 Ley 24.240` y `art. 988 CCyCN` .
- Afectación a la inviolabilidad de la persona humana y su dignidad (`art. 51 CCyCN`).
- Supuestos en que la ley expresamente impida la limitación convencional de la responsabilidad.

En tales casos excluidos, la responsabilidad se rige por las reglas generales del derecho común.

14.6 Responsabilidad por brechas de ciberseguridad

Ante una brecha de seguridad que comprometa datos personales tratados por el responsable, éste asume frente al titular afectado las siguientes obligaciones:

- Notificación al titular dentro de las **72 horas** de conocida la brecha (ver Sección 13).
- Notificación a la AAIP cuando la severidad lo amerite conforme Res. AAIP 47/2018.
- Adopción inmediata de medidas mitigadoras.
- Publicación de informe post-mortem con causa raíz y correcciones implementadas.

La responsabilidad del responsable por la brecha se evaluará conforme al **estado del arte en materia de seguridad informática** al momento del hecho. La acreditación del cumplimiento de las medidas previstas en la Res. AAIP 47/2018 (nivel medio) constituye prueba del cumplimiento de la diligencia exigible.

14.7 Prescripción

Los plazos de prescripción aplicables a las acciones derivadas del presente vínculo son los establecidos en el Código Civil y Comercial:

- **Acciones por responsabilidad civil derivada del uso del servicio:** tres (3) años, computados desde que la acción puede ser ejercida (`art. 2561, segundo párrafo, CCyCN`).
- **Acciones derivadas de relaciones de consumo por daños:** idéntico plazo de tres (3) años (`art. 2561 CCyCN`), sin perjuicio de las disposiciones del art. 50 Ley 24.240, cuya vigencia actual aplica a sanciones administrativas.
- **Acciones de daños punitivos:** se rigen por el plazo de la acción principal (`art. 52 bis Ley 24.240`).
- **Reclamos administrativos ante AAIP:** conforme los plazos específicos del procedimiento administrativo aplicable.

15. Obligaciones del usuario e indemnidad del responsable

15.1 Obligaciones del usuario

El usuario se obliga a:

- **Usar el servicio conforme a derecho**, sin incurrir en conductas tipificadas como delito, contravención o infracción administrativa.
- **Suministrar información veraz y actualizada** al momento del registro y durante la relación, especialmente en cuanto a matrícula profesional, tomo/folio y datos personales.
- **Custodiar diligentemente sus credenciales de acceso**, no compartirlas, y notificar al responsable dentro de las 24 horas de detectada cualquier intrusión o uso indebido de su cuenta.
- **No utilizar el servicio** para el tratamiento de datos sensibles (`art. 7 Ley 25.326`) en volumen masivo o estructural, sin contar con el consentimiento expreso del titular y haber cumplido con la registración ante AAIP.
- **Respetar su propio deber de secreto profesional** en cuanto al manejo de información amparada por secreto abogado-cliente (`art. 58 Ley 5.177 PBA` , `art. 7 inc. c Ley 23.187 CABA` , `art. 156 CP`).
- **No realizar ingeniería inversa**, descompilación ni extracción no autorizada del código ni de los datos del servicio, salvo en los casos permitidos por ley.
- **No realizar accesos indebidos** a sistemas judiciales o de terceros valiéndose de la herramienta, bajo apercibimiento de las sanciones previstas en los arts. 153 bis y concordantes del Código Penal.
- **Mantener actualizado** el software del dispositivo (sistema operativo, navegador, antivirus) dado que buena parte de las medidas de seguridad del servicio dependen de la seguridad del entorno de ejecución controlado por el usuario.
- **Notificar al responsable** cualquier falla, defecto, vulnerabilidad o comportamiento anómalo detectado.

15.2 Conductas prohibidas

Queda expresamente prohibido al usuario:

- Utilizar el servicio con cuentas falsas, suplantando identidad de otro profesional o declarando

matrículas no vigentes.

- Introducir, a sabiendas, datos falsos, maliciosos o contrarios a la ley.
- Realizar carga masiva automatizada no autorizada (scraping abusivo) que comprometa el funcionamiento del servicio.
- Utilizar el servicio para actividades vinculadas con delitos contra el honor, daños, extorsión, amenazas, grooming, pornografía infantil u otros tipos penales.
- Redistribuir, sublicenciar o comercializar funcionalidades del servicio sin autorización expresa y escrita del responsable.
- Comprometer la seguridad del servicio mediante ataques, exploits, inyecciones o cualquier técnica ofensiva.

El incumplimiento de estas obligaciones habilita al responsable a **suspender o cancelar la cuenta** de inmediato, sin perjuicio de las acciones civiles y penales que pudieren corresponder.

15.3 Indemnidad del responsable

El usuario se obliga a mantener **indemne** al responsable, sus directivos, colaboradores y proveedores, frente a toda reclamación, demanda, acción judicial o administrativa que terceros (incluyendo clientes del usuario profesional, colegas, contrapartes procesales o autoridades) promovieren como consecuencia de:

- Conductas del propio usuario contrarias a estos términos o a la ley.
- Violaciones al deber de secreto profesional por parte del usuario profesional.
- Uso de la herramienta para finalidades distintas de las aquí previstas.
- Incumplimientos del usuario a sus propias obligaciones profesionales (plazos procesales, asesoramiento, formas procesales, etc.) que el usuario pretendiere atribuir indebidamente al funcionamiento del servicio.

La indemnidad comprende gastos de representación, costas judiciales, honorarios de letrados, así como sumas que el responsable debiera abonar en concepto de capital, intereses y multas.

15.4 Cesación del vínculo

El vínculo puede cesar por:

- **Decisión del usuario**: dando de baja la cuenta en cualquier momento, sin causa ni preaviso, por la vía técnica provista o por solicitud a privacidad@argentinalitigia.com.
- **Decisión del responsable**: en caso de incumplimiento grave del usuario a estos términos, previa intimación fehaciente, salvo casos que por su gravedad justifiquen la cancelación inmediata (fraude, suplantación de identidad, actividad delictiva).
- **Cesación del servicio**: el responsable se reserva el derecho de discontinuar total o parcialmente el servicio, con preaviso de **noventa (90) días corridos** a los usuarios registrados, plazo durante el cual estos podrán exportar sus datos y ejercer los derechos ARCO (`art. 16 Ley 25.326`).

16. Ley aplicable y jurisdicción

El presente documento se rige por las leyes de la **República Argentina**. Para toda cuestión judicial derivada del uso del servicio, las partes se someten expresamente a la jurisdicción de los **tribunales ordinarios del Departamento Judicial de La Plata, Provincia de Buenos Aires**, con exclusión de cualquier otro fuero o jurisdicción que pudiera corresponder.

Sin perjuicio de lo anterior, el usuario que revista el carácter de **consumidor o usuario** en los términos de la Ley 24.240 conserva la facultad de demandar ante el juez del lugar de celebración del contrato, del cumplimiento de las obligaciones, del lugar donde se encuentre la cosa o servicio, o del domicilio del demandado, a su elección (`art. 1109 CCyCN`). En las relaciones de consumo, las cláusulas que pretendan limitar esta competencia son ineficaces.

En materia específica de protección de datos personales, resulta competente la **Agencia de Acceso a la Información Pública (AAIP)**, organismo nacional con sede en Av. Pte. Julio A. Roca 710, CABA, como autoridad administrativa de aplicación (`art. 29 Ley 25.326`).

17. Contacto del responsable

Canales oficiales

Cuestiones de privacidad y datos personales:
privacidad@argentinalitigia.com

Reporte de vulnerabilidades de seguridad:
privacidad@argentinalitigia.com — asunto: `[SECURITY]`

Ejercicio de derechos ARCO:
privacidad@argentinalitigia.com — asunto: `DERECHOS ARCO`

Autoridad administrativa de aplicación (Ley 25.326):
Agencia de Acceso a la Información Pública — argentina.gob.ar/aaip

Documentos jurídicos relacionados

Política de Privacidad completa conforme Ley 25.326

Política de Privacidad