Versión N° 1.0
Última modificación: 25/06/2026

AILOG

Inteligencia Logistica

Política de Seguridad

Plataforma de logística con agentes de IA autónomos y supervisión humana

Clasificación:	**PÚBLICO**
Propietario:	Juan Emilio Dalvit
Revisión anual:	01/06/2027

1. NUESTRO COMPROMISO

AILOG, producto de **Bits0 S.R.L.**, es una plataforma de logística con agentes de inteligencia artificial y supervisión humana. Procesamos datos operativos críticos para la cadena de suministro de nuestros Clientes; por eso la seguridad de la información es un pilar de nuestro servicio.

Este documento resume, en lenguaje accesible, **cómo protegemos la información** en la Plataforma. Está pensado para publicarse en nuestro sitio web y para responder las preguntas de seguridad más frecuentes de Clientes y prospectos.

Para documentación técnica detallada (arquitectura, controles operativos y procedimientos internos), AILOG dispone de una **Política de Seguridad de la Información** completa, disponible en procesos comerciales o bajo acuerdo de confidencialidad (NDA).

2. QUÉ PROTEGEMOS

AILOG protege la **confidencialidad**, **integridad** y **disponibilidad** de:

- Los datos logísticos y operativos que cada Cliente carga o genera en la Plataforma.
- Las credenciales y configuraciones de acceso de usuarios autorizados.
- Las comunicaciones entre Clientes, la Plataforma y los servicios de terceros autorizados.

La información de cada Cliente se trata por defecto como **confidencial**. Solo el personal y los sistemas que la necesitan para operar el servicio pueden acceder a ella, conforme al principio de **mínimo privilegio**.

3. CÓMO ESTÁ CONSTRUIDA LA PLATAFORMA (RESUMEN)

AILOG opera sobre una **arquitectura cloud híbrida** diseñada para combinar rendimiento operativo con capacidades analíticas e inteligencia artificial:

- **Capa de aplicación:** interfaz web, APIs y paneles de administración, accesibles de forma segura por Internet.
- **Capa de datos e inteligencia artificial:** procesamiento analítico, agentes de IA y servicios de IA en infraestructura cloud de nivel empresarial.
- **Entornos separados:** desarrollo y producción operan de forma independiente, con dominios y configuraciones diferenciadas.
- **Integraciones controladas:** conexiones con proveedores externos solo mediante canales cifrados y autenticados.

No publicamos diagramas de arquitectura interna ni detalles de implementación en este documento. Esa información se comparte en due diligence comercial cuando corresponde.

4. CONTROLES DE SEGURIDAD

4.1 Cifrado

- **En tránsito:** todas las comunicaciones entre Clientes y la Plataforma utilizan **HTTPS/TLS 1.2 o superior**.
- **En reposo:** los datos se almacenan en proveedores cloud que aplican cifrado en reposo; los campos sensibles (contraseñas, tokens) se protegen adicionalmente a nivel de aplicación.
- **Credenciales:** las contraseñas de usuario se almacenan con algoritmos de hash seguros. No se guardan en texto plano.

4.2 Acceso e identidad

- Autenticación segura para usuarios de la Plataforma.
- **Autenticación multifactor (MFA)** para personal de AILOG y para usuarios con roles administrativos o de gestión crítica en la Plataforma.
- Revisión periódica de accesos internos; revocación inmediata al finalizar relaciones laborales o contractuales.
- Accesos administrativos a infraestructura sujetos a controles adicionales.

4.3 Aislamiento entre Clientes

Los datos de cada Cliente están **lógicamente aislados** de los de otros Clientes mediante identificadores de organización, controles de sesión, roles y permisos. AILOG implementa controles para prevenir el acceso cruzado no autorizado entre organizaciones (tenant isolation).

4.4 Seguridad de red

- Protección perimetral con servicios de DNS, proxy y mitigación de ataques (incluyendo DDoS y reglas de seguridad web).
- Firewall y hardening del servidor de aplicación.
- Servicios internos críticos no expuestos directamente a Internet.

4.5 Seguridad de red

- Integración de seguridad en el ciclo de vida del software (diseño, desarrollo, pruebas y despliegue).
- Prohibición de credenciales en código fuente.

- Despliegues en producción mediante pipeline automatizado y controlado.
- Gestión de vulnerabilidades con plazos de remediación según severidad.

4.6 Copias de seguridad y continuidad

AILOG mantiene procedimientos de respaldo, monitoreo de disponibilidad y recuperación acordes a la criticidad de cada componente. Los servicios de datos e inteligencia artificial se apoyan en infraestructura cloud con mecanismos de alta disponibilidad y resiliencia.

5. INTELIGENCIA ARTIFICIAL

AILOG utiliza agentes de inteligencia artificial para automatizar y optimizar procesos logísticos, siempre con posibilidad de supervisión humana.

Compromisos en materia de IA:

- Cada agente opera con **acceso acotado** a los datos y operaciones necesarias para su función.
- Las entradas y salidas de los agentes pasan por **validaciones** para reducir riesgos de uso indebido o respuestas fuera de parámetros.
- Los agentes registran sus ejecuciones para **auditoría** y seguimiento operativo.
- Cuando se utilizan modelos de IA de terceros, los datos del Cliente **no se usan para entrenar** esos modelos, conforme a los términos del proveedor y los acuerdos aplicables.
- Las configuraciones y flujos de trabajo de agentes desarrollados por AILOG se versionan y despliegan mediante procedimientos autorizados.

6. SUBPROCESADORES

AILOG trabaja con proveedores tecnológicos de confianza para operar la Plataforma. Los que procesan datos en nombre de AILOG están sujetos a evaluación de seguridad y a acuerdos contractuales (incluyendo DPA cuando corresponde).

Proveedor	Servicio
Snowflake	Almacenamiento, procesamiento analítico e inteligencia artificial
Vultr	Infraestructura de aplicación
Cloudflare	DNS, proxy y protección perimetral
GitLab	Repositorio de código e integración continua
SendGrid	Envío de correo transaccional

La lista puede actualizarse. Los Clientes pueden solicitar notificación de cambios relevantes conforme a sus acuerdos contractuales.

7. CUMPLIMIENTO NORMATIVO

AILOG opera alineado con la normativa de protección de datos aplicable en las jurisdicciones donde presta servicios:

- **Argentina:** Ley N° 25.326 de Protección de Datos Personales y Disposición 11/2006 de la AAIP.

- **Chile:** Ley N° 21.719 de Protección de Datos Personales y reglamentos asociados.

Además, nuestros controles se inspiran en marcos internacionales de referencia, entre ellos:

- ISO/IEC 27001:2022
- NIST Cybersecurity Framework (CSF) 2.0
- OWASP Top 10 y OWASP ASVS
- NIST AI RMF (gestión de riesgos de IA)

7.1 Transferencia Internacional de Datos

Parte del procesamiento puede realizarse en regiones fuera del país del Cliente. AILOG adopta las medidas contractuales y técnicas necesarias para garantizar un nivel adecuado de protección, incluyendo acuerdos de procesamiento de datos con proveedores cloud.

8. GESTIÓN DE INCIDENTES

8.1 Qué hacemos ante un incidente

Si confirmamos un incidente de seguridad que comprometa datos de un Cliente, AILOG:

1. **Contiene** el incidente y protege los datos afectados.
2. **Investiga** la causa y el alcance.
3. **Recupera** el servicio de forma controlada.
4. **Documenta** lecciones aprendidas y mejora los controles.

8.2 Notificación a Clientes

AILOG notificará al Cliente afectado dentro de las **72 horas** de confirmar un incidente que haya comprometido sus datos, conforme a las obligaciones legales aplicables (incluyendo la Ley 25.326 en Argentina).

La notificación incluirá, en la medida de lo posible: descripción del incidente, datos potencialmente afectados, medidas adoptadas y recomendaciones para el Cliente.

Cuando la ley lo exija, AILOG notificará también a las autoridades competentes en los plazos establecidos.

9. DIVULGACIÓN RESPONSABLE DE VULNERABILIDADES

AILOG valora los reportes responsables de la comunidad de seguridad.

Si descubrió una vulnerabilidad en la Plataforma:

1. Envíe un informe a **tau.support@bits0.com** con asunto **"Reporte de Vulnerabilidad"**.
2. Incluya descripción, pasos para reproducir e impacto potencial.
3. No se divulgue públicamente hasta que AILOG haya podido investigar y remediar (plazo orientativo: 90 días).
4. No acceda, modifique ni divulgue datos de Clientes durante la investigación.

AILOG se compromete a acusar recibo dentro de las **48 horas**, investigar el reporte y comunicar el resultado. No emprenderá acciones legales contra investigadores que actúen de buena fe conforme a estas directrices.

10. RESPONSABILIDAD DEL CLIENTE

La seguridad es un esfuerzo compartido. Cada Cliente es responsable de:

- Gestionar de forma segura las credenciales de acceso a la Plataforma.
- Configurar permisos adecuados para sus usuarios.
- Proteger los sistemas desde los que se integran con las APIs de AILOG.
- Notificar a AILOG ante sospecha de uso no autorizado de su cuenta.

11. DOCUMENTACIÓN ADICIONAL

Este resumen público complementa, pero no reemplaza, la documentación contractual de AILOG:

Documento	Disponibilidad
Términos y Condiciones (TOS)	Público
Política de Privacidad	Público
Acuerdo de Nivel de Servicio (SLA)	Contractual
Acuerdo de Procesamiento de Datos (DPA)	Contractual
Acuerdo de Trabajo de Seguridad	Bajo NDA o proceso comercial

12. CONTACTO

Bits0 S.R.L. - AILOG

Documento	Disponibilidad	Asunto Sugerido
Consultas generales de seguridad	tau.support@bits0.com	Consulta de Seguridad
Reporte de incidente	tau.support@bits0.com	Reporte de Incidente
Divulgación responsable	tau.support@bits0.com	Reporte de Vulnerabilidad
Documentación bajo NDA	tau.support@bits0.com	Solicitud PSI / Due Diligence

---

La seguridad de la información es responsabilidad de todos en AILOG. El cumplimiento de esta Política es obligatorio para todo el personal, contratistas y proveedores con acceso a los sistemas y datos de la empresa.

.