# AlphaTech · Seguridad y Cumplimiento

Alphatech Software Innovation Solutions S. de R.L. de C.V.

**Código:** ATSIS-VSR-2026.11-ES
**Clasificación:** Dossier Público de Evaluación de Proveedores

## Paquete de Seguridad, Resumen de DPA y Política de Retención

Documento preparado para áreas de Seguridad de la Información (CISO), Cumplimiento Normativo, Jurídico y Riesgo de Proveedores (TPRM) que evalúan la infraestructura de APIs de KYC, KYB y Prevención de Fraude de AlphaTech.

### 1. Infraestructura Certificada y Mapeo de Controles

> **Transparencia en Auditoría:** AlphaTech opera íntegramente sobre Amazon Web Services (regiones `us-east-1` y `mx-central-1`), cuya infraestructura física y de nube cuenta con certificaciones vigentes **SOC 1/2/3, ISO/IEC 27001, ISO 27017, ISO 27018 y PCI-DSS Nivel 1**. Los controles internos de aplicación y operación de AlphaTech están diseñados y mapeados conforme a los criterios **SOC 2 (Seguridad, Confidencialidad y Disponibilidad)** e **ISO/IEC 27001:2022 Anexo A**. Mientras avanzamos en nuestra certificación corporativa independiente, entregamos respuestas completas a cuestionarios **SIG Lite / CAIQ**, sesiones técnicas con Arquitectura y opción de despliegue aislado en VPC del cliente u On-Premise.

### 2. Resumen Ejecutivo del Anexo de Protección de Datos (DPA)

Todos nuestros contratos corporativos (disponibles en español e inglés) incorporan nuestro Anexo de Encargado de Tratamiento (DPA) alineado a la **LFPDPPP** y estándares internacionales de debida diligencia:

- **Roles Jurídicos Claros:** El Cliente actúa como *Responsable* del tratamiento (confirmando base legal o autorización del titular); AlphaTech actúa exclusivamente como *Encargado* ejecutando únicamente las validaciones instruidas vía API o Portal.
- **Limitación Estricta de Finalidad:** AlphaTech jamás comercializa, perfila ni reutiliza datos o resultados de un cliente para beneficio propio o de terceros.
- **Subencargados Autorizados:** Acotados a Amazon Web Services, Inc. (cómputo aislado y gestión criptográfica) y Cloudflare, Inc. (protección perimetral TLS/WAF).
- **Notificación de Incidentes:** Compromiso contractual de notificación por escrito en menos de **24 horas** ante cualquier incidente confirmado de seguridad.
- **Contratación Local o Transfronteriza:** Soporte para contratación desde México (CFDI 4.0 en MXN) o desde casas matrices en EE. UU., Canadá, Europa y LATAM (MSA/DPA en inglés e Invoice en USD).

### 3. Política de Retención, Procesamiento Efímero y Purga Criptográfica

| Tipo de Artefacto | Cifrado y Custodia | Ventana de Retención | Mecanismo de Disposición |
|---|---|---|---|
| **Payloads API REST** (Síncronos y Asíncronos) | Cifrado híbrido `AES-256-GCM` + llave pública `RSA-4096-OAEP` del cliente. | **0 días de PII en claro** en reposo (procesamiento en memoria). | Texto cifrado descifrable solo por la llave privada del cliente; expiración automática. |

| Tipo de Artefacto | Cifrado y Custodia | Ventana de Retención | Mecanismo de Disposición |
|---|---|---|---|
| **Archivos Batch CSV** (Entrada y Salida) | Carga por TLS 1.3 y archivo de salida cifrado con la llave pública del cliente. | **1 hora** tras finalizar el lote (o purga manual inmediata). | Eliminación automática en S3 (incluyendo archivo de entrada) al expirar ventana o al pulsar Purgar. |
| **Bitácora de Auditoría y Consumo** | Huellas irreversibles `HMAC-SHA256`; cero datos personales en claro en logs. | Vigencia contractual de auditoría. | Baja definitiva de tenant y llaves en máximo 15 días hábiles tras terminación. |
| **Modo Zero-Retention / On-Premise** | VPC dedicada del cliente o contenedores en perímetro propio. | **0 bytes** fuera de la red del cliente. | Gobernado al 100% por el KMS y las políticas internas de la institución. |

## 4. Controles Criptográficos y Resumen de Pruebas de Seguridad

La plataforma implementa controles en profundidad verificados frente al estándar **OWASP API Security Top 10 (2023)**:

| Dominio de Control | Implementación Técnica Verificable |
|---|---|
| **Seguridad en Tránsito y Borde** | TLS 1.3 obligatorio con HSTS, mitigación DDoS y WAF perimetral en Cloudflare, más listas blancas de IP (CIDR) opcionales por organización. |
| **Confidencialidad Extremo a Extremo** | Esquema híbrido con llave efímera `AES-256-GCM` envuelta mediante `RSA-4096-OAEP-SHA256`. AlphaTech nunca posee la llave privada del cliente. |
| **Integridad y Anti-Replay** | Validación de `X-API-KEY`, ventana temporal `X-TIMESTAMP` y firma digital `RSA-PSS`; notificaciones Webhook firmadas con `HMAC-SHA256` único por cliente. |
| **Aislamiento de Red y Secretos** | Subredes privadas en AWS VPC, conexión a base de datos vía RDS Proxy con TLS estricto, permisos IAM de mínimo privilegio y rotación automática sin caída en AWS Secrets Manager. |
| **Gestión de Vulnerabilidades y Pentest** | Análisis continuo de código y dependencias, endurecimiento de imágenes de contenedor y pruebas periódicas de seguridad API sobre autenticación, autorización por tenant (BOLA), inyección y replay (**0 hallazgos Críticos o Altos abiertos**). |
| **Control de Acceso en Portal** | Roles granulares (RBAC), Segundo Factor de Autenticación (MFA TOTP), límites de consumo mensual por usuario y bitácora administrativa inmutable. |

## 5. Contacto de Arquitectura y Revisión de Proveedores

¿Tu área de Compliance o Compras requiere firmar NDA bilateral, revisar plantillas completas de MSA + DPA (ES/EN) o enviar su cuestionario institucional de evaluación de seguridad?

- **Mesa de Seguridad y Arquitectura:** info@alphatechsis.com (Asunto: *Revisión de Seguridad / Due Diligence*)
- **Centro de Seguridad Web:** https://alphatechsis.com/seguridad/
- **Accesibilidad Digital WCAG 2.1 AA:** Navegación por teclado verificada y contraste ≥ 4.5:1 en interfaz pública.

© 2026 Alphatech Software Innovation Solutions S. de R.L. de C.V.