

Especificación Técnica de Arquitectura & Seguridad

AI Hunter Agent · Plataforma de Inteligencia Comercial B2B (O&G, Minería e Infraestructura) · Next.js / TypeScript / Node.js · Vercel · Evaluación: Corporate IT & Security Review · Actualizado 26/08/2026

Clasificación de riesgo (Vendor Risk Assessment): BAJO (Low-Risk SaaS). La plataforma opera como motor analítico sobre información pública oficial (OSINT / Datos Abiertos del Estado). No requiere acceso a redes internas corporativas, no se conecta a ERPs transaccionales del cliente ni almacena secretos comerciales confidenciales del cliente.

1. RESUMEN EJECUTIVO Y ALCANCE

AI Hunter Agent es una solución SaaS de prospección e inteligencia de mercado para sectores industriales de capital intensivo (Energía, Oil & Gas, Minería e Infraestructura). Monitorea y procesa novedades del Boletín Oficial (BORA), registros regulatorios de la Secretaría de Energía, resoluciones de transporte/midstream y compras públicas, consolidando mutaciones de activos físicos en señales comerciales accionables.

2. ARQUITECTURA DE SOFTWARE E INFRAESTRUCTURA

- **Frontend & API:** Next.js (React) con tipado estricto en TypeScript. Serverless Functions (Node.js) con instancias efímeras y escalado elástico, sin servidores permanentes expuestos.
- **Plataforma cloud & CI/CD (Vercel):** despliegues inmutables con compilación aislada, atomic deploys y rollback instantáneo; red global Anycast; entornos Development / Preview / Production separados con variables de entorno independientes.

3. FLUJO DE DATOS Y PIPELINE DE INGESTA

[Fuentes públicas/regulatorias] → [Conectores modulares] → [Diff & Roll-up Engine] → [Almacenamiento seguro] → [Interfaz corporativa]

Componente	Implementación técnica	Garantía operativa
Conectores ontológicos	Micro-parsers tipados que extraen metadatos estructurados (operadores, diámetros, trazas).	Clasificación taxonómica estricta: midstream_pipeline, upstream_block, mining_infrastructure.
Idempotencia estricta	Firma hash SHA-256 única por acto administrativo o evento de pozo.	Cero duplicados ante reintentos de jobs o ejecuciones cron recurrentes.
Anti-flapping	Ventanas temporales de confirmación para cambios de estado de activos físicos.	Elimina ruido por fluctuaciones transitorias o backfills de padrones públicos.
Diff & Roll-up Engine	Diferencias entre snapshots del regulador, agregadas a nivel bloque.	Transforma 2.000+ cambios de pozos individuales en una única señal consolidada.

4. IDENTIDAD, ACCESOS Y AISLAMIENTO MULTI-TENANT

- **Autenticación:** Supabase Auth (GoTrue) con credenciales individuales y hashing unidireccional bcrypt. **SSO corporativo (SAML 2.0 / OIDC — Entra ID, Google Workspace) disponible a pedido** para despliegues enterprise.
- **Control de acceso por roles:** separación de privilegios entre administración de plataforma, staff de operaciones y usuarios de cada organización cliente.
- **Aislamiento multi-tenant:** particionamiento lógico estricto por organización a nivel de base de datos, con políticas de Row-Level Security (RLS) sobre las tablas de datos de contacto para impedir fuga cruzada entre empresas.

5. CIFRADO, ALMACENAMIENTO Y SECRETOS

- **En tránsito:** HTTPS/TLS en todo el tráfico externo, con HSTS forzado (2 años, incl. subdominios).
- **En reposo:** base de datos relacional gestionada (Supabase / AWS) con cifrado AES-256 en almacenamiento y backups.
- **Zero hardcoded secrets:** credenciales y claves API en el almacén cifrado de variables de entorno de la infraestructura serverless; nunca en el código ni en el navegador.

6. SEGURIDAD DE RED Y PERÍMETRO

Vector / capa	Mecanismo de protección
Perímetro	Firewall de plataforma (Vercel) con mitigación DDoS L3/L4/L7 y protección contra bots maliciosos en la capa Edge.
Endpoints internos (/api/*)	Ingesta y cron protegidos por tokens criptográficos de servicio verificados server-side (no accesibles desde el navegador); las descargas de datos exigen aprobación firmada HMAC.

Vector / capa	Mecanismo de protección
Cabeceras HTTP	Inyección automática en toda respuesta: Content-Security-Policy, X-Frame-Options: DENY, X-Content-Type-Options: nosniff, Referrer-Policy y Permissions-Policy restrictiva.

7. AUDITORÍA, DISPONIBILIDAD Y CONTINUIDAD

- **Trazabilidad:** registro de accesos a fichas de contacto y actividad sobre endpoints críticos; telemetría del pipeline de ingesta (estado de conectores, tiempos, errores).
- **Disponibilidad:** objetivo operativo de 99,9% sobre infraestructura serverless gestionada; SLA contractual disponible según acuerdo comercial.
- **Backups:** copias de seguridad automáticas diarias con retención programada.

8. MATRIZ DE RESPUESTAS PARA EL CUESTIONARIO DE IT / CISO

Pregunta típica de auditoría IT	Respuesta técnica oficial
¿Requiere instalar agentes en servidores del cliente?	No. SaaS 100% cloud basado en navegador, sin instalación local ni permisos en la intranet del cliente.
¿Qué datos del cliente se almacenan?	Credenciales de acceso de sus usuarios y configuraciones de búsqueda/alertas. No se ingesta información financiera ni operativa interna del cliente. Los datos de contacto B2B se tratan según la política de privacidad (Ley 25.326): app.aihunteragent.com/legal .
¿Cómo se separan los datos entre empresas?	Aislamiento lógico estricto por organización a nivel de base de datos, con Row-Level Security y autorización por sesión.
¿Cómo se gestionan contraseñas y accesos?	Hashing unidireccional bcrypt vía Supabase Auth; SSO corporativo (SAML/OIDC) disponible a pedido.

Conclusión de cumplimiento: AI Hunter Agent sigue las mejores prácticas de la industria en desarrollo seguro, cifrado y aislamiento multi-inquilino, con una superficie de ataque mínima y un perfil de riesgo bajo para el área de Seguridad de la Información corporativa. Versión web actualizada: app.aihunteragent.com/legal/arquitectura · Consultas: privacidad@adsmartm.com