2026

SAPIENS – SNA

Sistema de Análisis de Redes y Vínculos V3.1

SAPIENS INTELLIGENCE CONSULTING GROUP

DIVISIÓN DE INTELIGENCIA ESTRATÉGICA.

MÉXICO, Febrero 2026

SAPIENS - SNA

Sapiens Networking Analyzer V3.1

1. PROPUESTA DE VALOR

El Desafío Operacional

Las organizaciones de seguridad e inteligencia enfrentan una brecha crítica en el análisis de redes criminales: mientras la información sobre actores, vínculos financieros y estructuras organizacionales se multiplica exponencialmente, las herramientas disponibles se limitan a software de análisis estático que requiere alimentación manual, no integra fuentes abiertas automáticamente, y carece de capacidades predictivas.

El resultado: investigaciones que toman semanas para mapear una red, perfiles de objetivos incompletos por falta de tiempo, y análisis de amenazas que llegan tarde para la toma de decisiones. La brecha entre la velocidad del crimen organizado y la capacidad analítica de las instituciones se amplía cada día.

SAPIENS NETWORKING ANALYZER–SNA

SNA es una plataforma de análisis de redes y perfilamiento OSINT potenciada por inteligencia artificial multi-modelo, diseñada específicamente para investigaciones de entorno complejos multifactoriales. Integra seis módulos analíticos que permiten mapear redes completas, generar perfiles OSINT de 8 dimensiones, evaluar amenazas con indicadores de alerta temprana, y proyectar escenarios —todo en una sola plataforma, en español nativo, en minutos.

Capacidad	Beneficio
Análisis de Redes (Link Analysis)	Mapeo interactivo de vínculos entre personas, organizaciones, empresas y células con validación OSINT automatizada
OSINT Profiler (8 dimensiones)	**Perfilamiento integral:** datos generales, estatus legal, estructura financiera, vínculos, perfil operacional, hitos, evaluación de riesgo y fuentes
IA Multi-Modelo (3 motores)	**NOUS** (Claude/Anthropic), **LOGOS (GPT-4o/OpenAI)** y **GEMINI (Google)** para análisis triangulado y eliminación de sesgos
Evaluación de Amenazas e I&W	Hipótesis competidoras, niveles de probabilidad, indicadores de alerta temprana con priorización automatizada
Cono de Plausibilidad	Proyección de escenarios con probabilidades, factores determinantes e indicadores de seguimiento por escenario
Código Admiralty (A1-F6)	Sistema de evaluación de confiabilidad de fuentes y veracidad de información conforme a estándares NATO/OTAN
Integración CSINT	Posibilidad de incorporación de fuentes cerradas de inteligencia (HUMINT, SIGINT, clasificadas) al análisis de red
Exportación PDF Profesional	Reportes con clasificación de seguridad, redes de vínculos, perfiles y análisis listos para diseminación

2. MÓDULOS ANALÍTICOS

SAPIENS-SNA integra seis módulos especializados que cubren el ciclo completo de análisis de redes de vínculos, desde la recolección OSINT hasta la proyección de escenarios:

2.1 RED — Análisis de Vínculos

Función	Descripción
Grafo interactivo	Visualización de nodos (personas, organizaciones, empresas, células, finanzas) con vínculos tipificados (mando, operacional, financiero, lavado, protección, soborno)
Generación OSINT automatizada	Ingreso de un nombre o entidad y generación automática de red de vínculos con fuentes verificadas mediante búsqueda en fuentes abiertas
Modos de análisis	OSINT (fuentes abiertas), CSINT (fuentes cerradas) y OSINT+CSINT (análisis combinado para máxima cobertura)
Expansión de red	Ampliación progresiva de la red: cada nodo puede expandirse para descubrir nuevos vínculos y conexiones nuevas
Código Admiralty	Cada nodo y vínculo clasificado con código A1–F6 de confiabilidad de fuente y veracidad de información

2.2 PROFILER — Perfilamiento OSINT de 8 Dimensiones

Estructura de Perfil de Inteligencia

Sección	Dimensión	Contenido
S1	Datos Generales	Nombres, apellidos, alias, nacionalidad, fecha de nacimiento
S2	Estatus Legal	Estado legal actual, procesos activos, órdenes de aprehensión, sanciones
S3	Estructura Financiera	Empresas vinculadas, propiedades, activos identificados, flujos financieros
S4	Vínculos y Estructura	Asociados clave, organizaciones vinculadas, estructura jerárquica
S5	Perfil Operacional	Modus operandi, zonas de operación, capacidades identificadas
S6	Hitos Históricos	Cronología de eventos relevantes, detenciones, operativos, actividades documentadas
S7	Evaluación de Riesgo	Nivel de riesgo (CRÍTICO/ALTO/MEDIO/BAJO), resumen ejecutivo de amenaza
S8	Fuentes OSINT	URLs verificadas, clasificación Admiralty de confiabilidad, fecha de consulta

2.3 ANÁLISIS — Evaluación de Amenazas e I&W

Componente	Aplicación
Matriz de Amenazas	Evaluación con niveles (CRÍTICO, ALTO, MEDIO, BAJO), tendencia (↑→↓), sector y probabilidad porcentual
Hipótesis Competidoras (ACH)	Generación y evaluación de hipótesis alternativas con nivel de confianza y estado (activa/descartada/confirmada)
Indicadores y Alerta Temprana	Sistema I&W con priorización P1–P3, estados de alerta y monitoreo continuo de señales
Análisis ejecutivo con IA	Síntesis automatizada que integra amenazas, hipótesis e indicadores en un análisis coherente para tomadores de decisiones

2.4 Cono de Plausibilidad y Escenarios

Capacidad	Descripción
Escenarios probabilísticos	Generación de múltiples escenarios con porcentaje de probabilidad basado en evidencia disponible
Factores determinantes	Identificación de variables clave que condicionan cada escenario con nivel de certeza
Indicadores de seguimiento	Señales específicas por monitorear para detectar hacia cuál escenario evoluciona la situación

3. TECNOLOGÍA Y ARQUITECTURA

3.1 Arquitectura Multi-IA de Clase Mundial

SAPIENS-SNA implementa una arquitectura única de tres motores de inteligencia artificial que trabajan en coordinación, garantizando análisis triangulado, eliminación de sesgos algorítmicos y máxima cobertura analítica:

Motor	Plataforma	Rol en SNA
NOUS	Claude Sonnet 4 (Anthropic)	Motor principal: OSINT, generación de redes de vínculos, análisis ACH, evaluación de amenazas e I&W. Máxima precisión analítica.
LOGOS	GPT-4o (OpenAI)	Síntesis estratégica y perspectiva alternativa: contraste de hipótesis, visión complementaria para eliminación de sesgos.
GEMINI	Gemini 2.0 Flash (Google)	Análisis visual y síntesis multimodal: complementa el análisis de red con capacidades de procesamiento de imágenes y documentos.

3.2 Características de Seguridad

- Sistema de selección de clasificación de seguridad multinivel (No Clasificado a Ultrasecreto)
- Código Admiralty (A1–F6) en cada nodo, vínculo y perfil para trazabilidad de fuentes
- Exportación PDF con marca de agua de clasificación y metadatos de seguridad
- Arquitectura cloud con encriptación en tránsito y en reposo
- Sin almacenamiento de datos sensibles en dispositivos locales
- Opción de despliegue en infraestructura propia del cliente

4. USUARIOS OBJETIVO Y CASOS DE USO

4.1 Perfiles de Usuario

Usos y Aplicaciones por Sector

Sector	Usuario / Aplicación
Gobierno Federal	Unidades de inteligencia civil/militar, análisis de redes de delincuencia organizada transnacional, amenazas a seguridad nacional
Gobiernos Estatales	Secretarías de seguridad, análisis de células criminales locales, mapeo de estructuras de narcotráfico
Fiscalías / Procuradurías	Análisis criminal complejo, investigación patrimonial, lavado de dinero, perfilamiento de objetivos
Fuerzas Armadas	Inteligencia naval y militar, mapeo de organizaciones criminales, análisis de amenazas emergentes
Sector Privado	Due diligence, análisis de riesgo de contraparte, detección de fraude corporativo, protección ejecutiva
Organismos Internacionales	Análisis de redes transnacionales, financiamiento del terrorismo, tráfico de personas

5. BENEFICIOS OPERACIONALES

5.1 Beneficios Cuantitativos

Métrica	Impacto
⏱ Tiempo de análisis de red	Reducción del 90% (de semanas a horas para mapeo completo de organización criminal)
🔍 Perfilamiento OSINT	8 dimensiones automatizadas por objetivo vs. investigación manual fragmentada
🧠 Motores de IA	3 modelos trabajando en paralelo: análisis triangulado, eliminación de sesgos algorítmicos
📄 Documentación	Exportación PDF profesional instantánea con clasificación de seguridad
💰 Costo total	90% menor vs. soluciones enterprise internacionales (Palantir, Recorded Future)

5.2 Beneficios Cualitativos

- Estandarización del proceso de análisis de redes en la organización
- Eliminación de sesgos mediante triangulación de tres motores de IA independientes
- Trazabilidad completa de fuentes con Código Admiralty NATO/OTAN en cada dato
- Transferencia de conocimiento: analistas menos experimentados producen análisis de nivel senior
- Integración OSINT + CSINT en una sola plataforma, eliminando silos de información
- Idioma español nativo con contexto operacional de México y Latinoamérica

6. ECOSISTEMA SAPIENS

SAPIENS-SNA forma parte de un ecosistema integrado de herramientas de inteligencia desarrolladas por Sapiens Intelligence:

Las plataformas son complementarias y pueden integrarse para cubrir el ciclo completo de inteligencia: SIA para el análisis estratégico, SNA para el mapeo de redes y perfilamiento, TAC para la planificación táctica, e INA para la explotación de fuentes humanas.

SAPIENS INTELLIGENCE CONSULTING GROUP

Consultoría Estratégica en Inteligencia y Seguridad

Solicite una demostración personalizada

www.sapiensintel.com

Desarrollado en colaboración con *Claude by Anthropic y Google Gemini*
