NEXO IQ

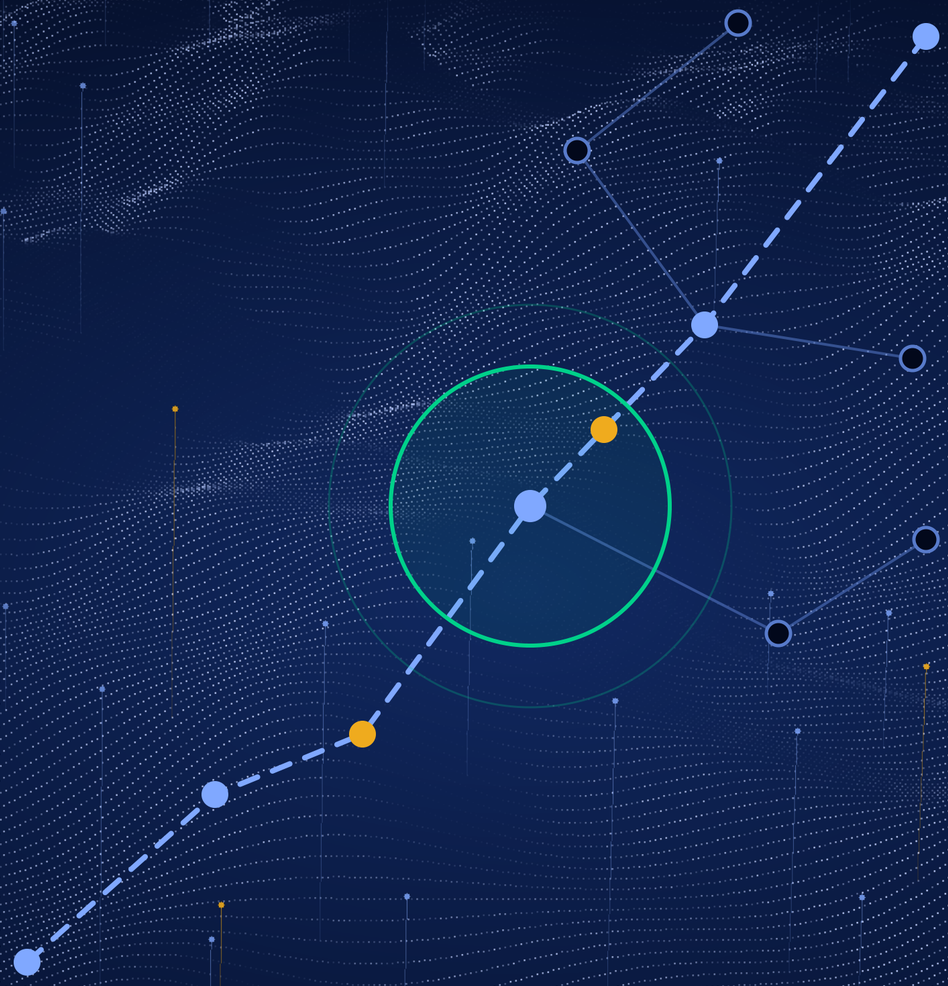
PRESENTACIÓN EJECUTIVA

DEFENSA E INTELIGENCIA

Inteligencia fusionada para la defensa.

Soberana, compartimentada y auditable.

Del reporte de campo, el documento incautado y el registro de comunicaciones a un producto de inteligencia validado: en red aislada, con IA local y bajo control legal.



Fuerzas militares · Inteligencia estratégica · Policía antinarcóticos · Control fronterizo y marítimo · Análisis financiero

RESUMEN EJECUTIVO

Inteligencia validada, bajo control de la institución

QUÉ ES

Fusión de inteligencia

Reportes de campo, documentos incautados, comunicaciones y listas oficiales en un solo sistema, con cada conclusión trazada hasta su fuente.

QUÉ GARANTIZA

Soberanía y control legal

Opera en la infraestructura de la institución, incluso en red aislada, con IA local, compartimentación por fuente y registro inmutable.

QUÉ ENTREGA

Inteligencia y evidencia

Informe validado para el mando y paquete probatorio firmado para judicializar, sin rehacer el análisis.

1 **Demostración**
Con un caso SIMULADO de la región.

2 **Piloto de 30 días**
Sobre un caso real, en la infraestructura de la institución.

3 **Acuerdo Empresarial**
Anual, directo o a través de un integrador local.

EL DESAFÍO OPERACIONAL

La amenaza es una red; la información, no

01 Información en silos

Cada fuerza, unidad y agencia guarda su parte. Los vínculos entre estructuras, rutas y financiadores solo aparecen cuando alguien cruza todo a mano.

02 Ventanas de decisión cortas

Una ruta cambia en días. Si el análisis toma semanas, el producto de inteligencia llega tarde al mando.

03 Soberanía del dato

Plataformas extranjeras procesan información clasificada fuera de la jurisdicción nacional, con dependencias tecnológicas que el Estado no controla.

04 Control y rendición de cuentas

Toda capacidad de inteligencia está bajo escrutinio legal y político. La institución debe probar qué se consultó, quién, cuándo y con qué autorización.

CICLO DE INTELIGENCIA

Del dato crudo al producto validado, en un solo sistema

Trazabilidad de punta a punta: cada conclusión llega hasta su fuente.

1

Obtención

Reportes, documentos incautados, comunicaciones, listas y fuentes abiertas autorizadas.

2

Fusión

Entidades únicas a partir de muchas fuentes, con procedencia por dato y sin mezclar compartimentos.

3

Análisis

Redes, rutas, zonas, co-ocurrencia y línea de tiempo; agentes de IA que proponen.

4

Validación

Compuertas: fuentes independientes, vigencia y revisión por otra persona.

5

Producto

Informe para el mando o paquete probatorio firmado para judicializar.

DOBLE RESULTADO

Dos salidas del mismo trabajo.

PARA EL MANDO

Inteligencia para decidir hoy

Informe validado, con cada conclusión trazada hasta su fuente.

PARA LA JUSTICIA

Evidencia que se sostiene mañana ante un juez

Paquete probatorio firmado, sin rehacer el análisis.

Cadena de custodia alineada con ISO/IEC 27037 · Paquete firmado digitalmente (Ed25519)



Registro de custodia en la plataforma: cadena íntegra.

POR QUÉ NEXO

Diseñada desde el inicio para entornos clasificados

PILAR 1

Soberanía total

En la infraestructura de la institución, incluso en red aislada (air-gap).

IA local, sin salida a internet. Actualizaciones por paquete firmado.

Código fuente en depósito de garantía (escrow).

PILAR 2

Necesidad de saber

Clasificación por propiedad y habilitación por usuario.

Casos restringidos y compartimentación por fuente.

Lo no habilitado no aparece en búsquedas, conteos ni grafo.

PILAR 3

Control legal demostrable

Cada acción sensible exige base legal.

Registro inmutable, hash-encadenado.

Ante un órgano de control, se prueba el uso consulta por consulta.

Protege a la institución y al analista: se puede usar con intensidad porque cada paso queda justificado y verificable.

MISIONES

Un núcleo analítico para las amenazas de la región

ANTINARCÓTICOS

Narcotráfico y economías ilícitas

Redes de producción, acopio y salida; laboratorios, pistas, puertos y corredores; minería ilegal y contrabando.

GRUPOS ARMADOS

Estructuras armadas organizadas

Mandos, integrantes, zonas de influencia, designaciones oficiales y relaciones, tal como las declara cada fuente.

CONTROL TERRITORIAL

Fronteras, ríos y litoral

Rutas terrestres, fluviales y marítimas; presencia por celda en corredores y geocercas sobre puntos de cruce.

FINANZAS

Financiación de la amenaza

Testaferros, empresas pantalla, transferencias y cruces con listas de sanciones; vigilancia de cambios en las entidades.

COORDINACIÓN

Fusión interagencial

Un espacio común entre fuerzas y agencias, compartimentado por fuente y por caso, sin entregar el control del dato propio.

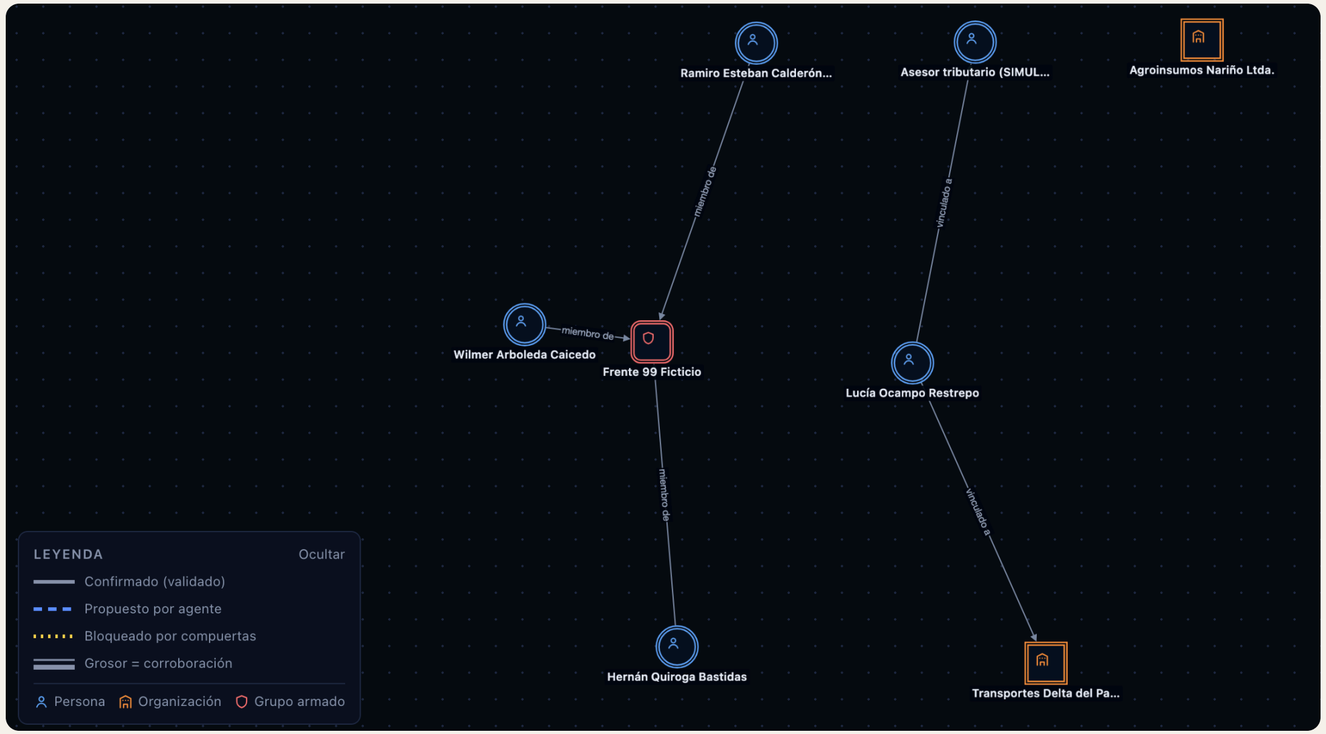
JUSTICIA

Apoyo a la judicialización

Del producto de inteligencia al caso: hallazgos validados con cita de su fuente y paquete probatorio firmado.

CONSOLA DE INVESTIGACIÓN

Todo el caso en una pantalla



Grafo del caso en la plataforma: vínculos confirmados, propuestos por agente y bloqueados por compuertas. Datos SIMULADOS.

Agentes proponen, personas deciden

Documental, telefonía, societario, listas y geotemporal trabajan en paralelo. Nada llega al grafo sin validación humana.

Compuertas configurables

Mínimo de fuentes independientes, antigüedad y revisión jurídica por otra persona.

Lectura del grafo sin ambigüedad

Sólido: validado. Discontinuo: propuesto. Punteado: bloqueado. El grosor indica corroboración.

Prioridad explicable

Cada hallazgo muestra por qué está arriba: relevancia, corroboración y novedad.

INTELIGENCIA ESPACIO-TEMPORAL

Quién estuvo dónde, cuándo y con quién

Zonas a la medida

Círculo, polígono, corredor a lo largo de una ruta o zona anclada a un hecho conocido. También capas KML, KMZ y GeoJSON de la institución.

Geocercas con vencimiento

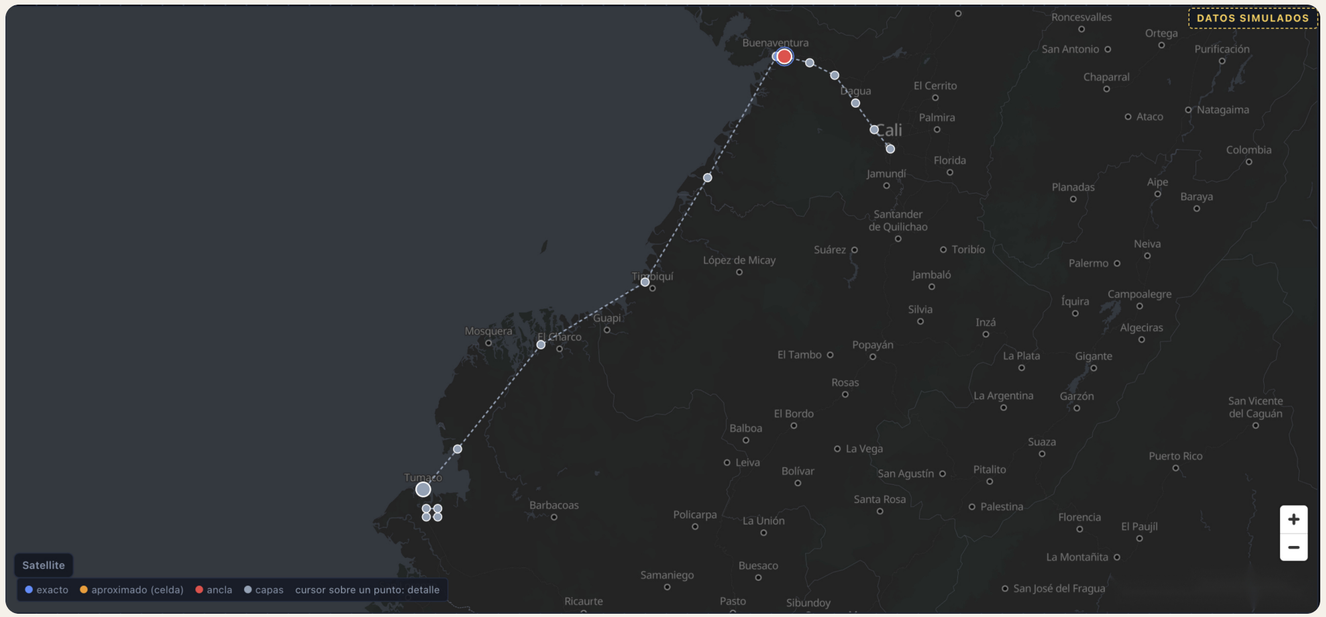
Avisan cuando un evento nuevo cae en la zona. Vigencia máxima de 90 días, renovable con motivo y base legal.

Co-ocurrencia

Pares que coinciden en lugar y momento, o que se comunican.

Precisión honesta

La presencia por celda se marca aproximada: ubica la antena, no a la persona.



Corredor Buenaventura–Tumaco en la plataforma. Datos SIMULADOS.

FUENTES

Fusiona lo propio, lo interinstitucional y lo oficial

01	**Reportes y documentos**	Informes, actas y material incautado en PDF, imagen o DOCX bajo custodia, con OCR local. Extrae teléfonos, documentos, cuentas, personas y lugares con cita de página.
02	**Registros de comunicaciones**	Registros obtenidos legalmente, convertidos en eventos con hora y celda: contactos frecuentes, contactos en común y presencia.
03	**Listas y designaciones**	OFAC SDN, FBI Wanted y OpenSanctions en ficha unificada. Cada designación se registra tal como la declara la fuente; el sistema nunca etiqueta por su cuenta.
04	**Bases de cada fuerza**	CSV, Excel y SQL con mapeo declarativo, sin programar. Fusión de entidades explicable y reversible.
05	**Fuentes abiertas autorizadas**	Búsqueda de cuentas por usuario declarado, solo con orden vigente y salida controlada; los resultados son candidatos a validar.
06	**Registro de fuentes**	Cada fuente con organismo, instrumento legal, finalidad, clasificación, vigencia y habilitados. La fuente no habilitada no deja rastro.

INTELIGENCIA ARTIFICIAL CON CONTROL

La IA acelera; la decisión sigue siendo humana

Solo lectura

Los agentes consultan con los permisos de quien los lanzó. Su único efecto posible es proponer un hallazgo.

Nada inventado

Cada cita se verifica contra el texto literal de la página; lo que no existe en el documento se descarta.

Contenido como dato

Lo ingerido nunca se trata como instrucción: se aísla, y la salida del modelo se valida.

Costo bajo control

Tope de gasto por caso y registro completo de cada paso: qué consultó, qué concluyó y cuánto costó.

IA local, sin salida a internet

Un cliente de modelo con dos adaptadores: nube o modelo local en los servidores de la institución. En modo aislado (air-gap), todo sigue funcionando.

Asistente en lenguaje natural

Solo ve lo que el usuario puede ver y cita la procedencia de cada dato. Las acciones de escritura se proponen; nunca se ejecutan sin confirmación.



SEGURIDAD DE LA INFORMACIÓN

Compartimentación de verdad, no solo pantallas ocultas

ACCESO COMPARTIMENTADO

Clasificación por propiedad
Cada atributo declara su nivel; se redacta según la habilitación.

Compartimentos por fuente
La fuente no habilitada desaparece de búsquedas, conteos, grafo y fichas.

Casos restringidos
Quien no está asignado no ve el caso ni puede saber que existe.

Separación de funciones
Quien valida un hallazgo no puede hacer su revisión jurídica.

AISLAMIENTO TÉCNICO

Aislamiento en la base de datos
Segunda barrera por institución a nivel de base (row-level security).

IA sin fuga
El modelo solo ve lo que el usuario puede ver; lo ingerido nunca se trata como instrucción.

Pruebas de aislamiento
Prueba de penetración entre instituciones sobre todas las rutas de la API.

INTEGRIDAD Y OPERACIÓN

Registro inmutable
Cadena append-only hash-encadenada; cualquier alteración se detecta.

Instalación verificable
Paquete firmado; firma e integridad se verifican antes de cargarlo.

Respaldo y operación
Respaldos con verificación de integridad, monitoreo y chequeos de salud.

CONTROL LEGAL Y USO RESPONSABLE

Límites incorporados al producto, no a un manual

Base legal por acción

Ingesta de comunicaciones, geocercas, búsquedas en fuentes abiertas y cotejos exigen declarar la base legal. Sin ella, la acción no se ejecuta.

Órdenes con alcance

Cada orden declara qué habilita. Una orden para fuentes abiertas no habilita biometría: si el alcance no la cubre, el sistema falla cerrado.

Vigilancia con vencimiento

Las geocercas vencen a los 90 días como máximo. Renovar exige motivo y queda en el registro.

Biometría solo dirigida

Cotejo facial únicamente contra sujetos autorizados por orden. No hay búsqueda facial abierta sobre la población.

Sin etiquetas automáticas

El sistema no califica a nadie: registra la situación tal como la declara la fuente oficial, con su fecha y su enlace.

Ejercicio separado de la operación

Los datos de entrenamiento y demostración se marcan SIMULADO y nunca se cruzan con datos reales.

MODELO DE ENTREGA

Una capacidad completa, no solo una licencia

Para defensa e inteligencia, NEXO se entrega como Acuerdo Empresarial de capacidad.

Licencia institucional

Todos los módulos y usuarios ilimitados dentro de la entidad que firma.

Equipo dedicado

Ingenieros y analistas de soporte, con presencia en sitio y acuerdo de servicio 24/7.

Desarrollo a medida

Conectores a sistemas propios, nuevas fuentes y ajustes a la doctrina de la institución.

Capacitación y transferencia

Formación de analistas y administradores, manuales y ejercicios con datos SIMULADOS.

Continuidad

Código fuente en depósito de garantía (escrow) y apoyo a los procesos de acreditación.

Despliegue aislado

Instalación en red aislada con paquete firmado, IA local y operación sin internet.

1 **Demostración**
Con un caso SIMULADO de la región.

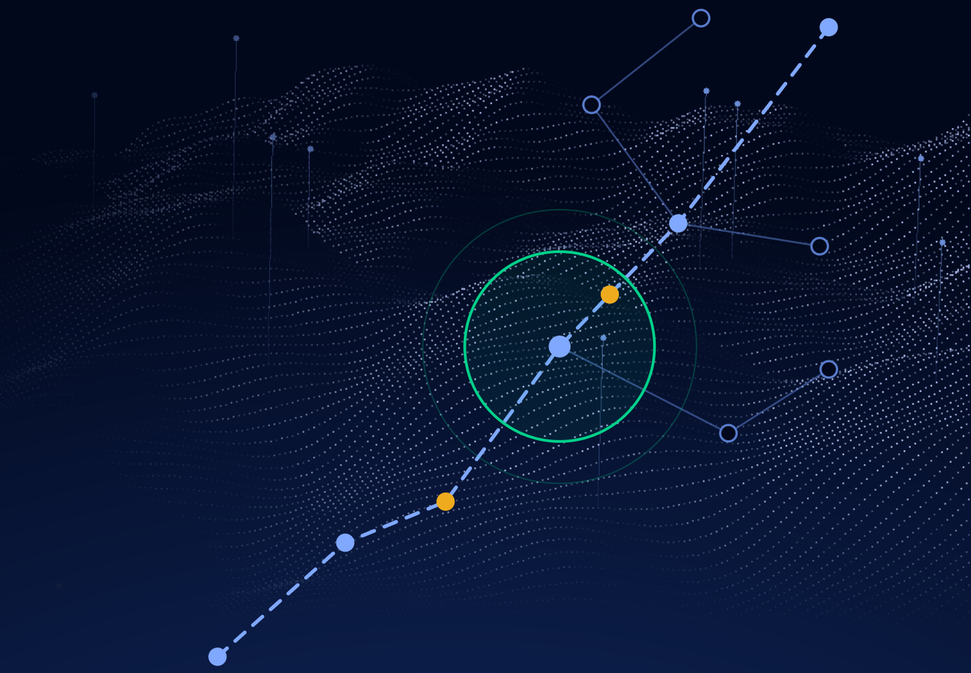
2 **Piloto de 30 días**
Sobre un caso real, en la infraestructura de la institución.

3 **Acuerdo Empresarial**
Anual, directo o a través de un integrador local.

DEMOSTRACIÓN RESERVADA

Véalo en un escenario de la región.

Demostración guiada de 30 minutos, de punta a punta y sin salida a internet, con datos 100 % SIMULADOS.



Corredor Buenaventura–Tumaco

Capas KML, búsqueda espacio-temporal por celdas y una geocerca que avisa en vivo.

Operación Marea

Expediente de 23 páginas, menciones con cita, hallazgos validados y Universo del caso.

Producto y prueba

Informe validado para el mando y paquete firmado con verificación de la cadena de custodia.

SOLICITE UNA DEMOSTRACIÓN RESERVADA

claudio@vectoraiq.dev www.vectoraiq.dev