



Seguridad Nacional

La seguridad nacional requiere de herramientas que permitan el análisis y el manejo de datos complejos y diversos. Para este caso Sirtech, VisuaLinks y DIG son herramientas invaluable para las Agencias nacionales en su misión de custodiar la seguridad de un país contra el Terrorismo y el crimen organizado, a nivel internacional.



Organismos de Seguridad Doméstica

Los organismos de seguridad doméstica, encargados de la lucha contra el crimen organizado o común, requieren de herramientas como Sirtech, DIG y VisuaLinks que ayudan a los investigadores nacionales, provinciales o locales, a descubrir relaciones que permitan develar casos criminales.



Industria y Comercio

Los sistemas SYSTECH VIGIA, Sirtech, VisuaLinks y DIG permiten, en las empresas dedicadas a la industria y el comercio, alcanzar las metas de productividad, identificar y exponer fraudes y ubicar posibles áreas para nuevos desarrollos de productos.

Combate del terrorismo



El terrorismo es una amenaza global que afecta la vida y comportamiento de las sociedades, ejecutando o amenazando con acciones devastadoras, las cuales, pueden incluir armas convencionales, biológicas, químicas, e incluso nucleares.

Hoy en día, el terrorismo también amenaza los recursos económicos y de información. La creciente dependencia respecto de las tecnologías de la información aumenta la vulnerabilidad ante ataques terroristas. El mayor acceso a la información y la centralización de elementos vitales de la infraestructura local, nacional y global, es una amenaza para la seguridad.

La investigación de los grupos terroristas exige la intercomunicación y colaboración entre organismos, con la capacidad de obtener y analizar datos de varias fuentes a fin de controlar, infiltrar y prevenir la actividad terrorista. El terrorismo es un acto premeditado que exige preparativos detectables, tales como transferencias de fondos, compra de elementos y movimientos de personas.

“La actividad de inteligencia es esencial para evitar los actos terroristas. El análisis cuidadoso y a tiempo, y la difusión de la información sobre los terroristas y sus actividades, mejorará la capacidad del gobierno para interferir y evitar actos terroristas, y para proporcionar avisos que sirvan al sector privado y a la población en general.”

- Presidente George W. Bush citado en “The Department of homeland Security” - www.whitehouse.org

La solución

Sirtech®, VisuaLinks® y Digital Information Gateway (DIG™) están concebidos para recuperar información en diferentes formatos y fuentes, mostrando actividad oculta y patrones de comportamiento.

Funcionalidades:

- Identificar Relaciones: mostrar interacciones y relaciones entre grupos terroristas y sus integrantes.
- Vincular a los miembros de los grupos: entender las estructuras formales e informales de la organización.
- Conectar redes: mostrar conexiones entre los miembros del grupo, individuos externos, otras organizaciones, lugares, recursos y redes de comunicación.
- Mostrar las operaciones: recursos compartidos, materiales e insumos necesarios para operaciones terroristas.
- Rastrear tecnologías: detectar las tecnologías utilizadas en las armas terroristas.
- Entender los comportamientos: rastrear y analizar las conductas grupales para detectar, en forma temprana, posibles amenazas.
- Vulnerabilidad de los recursos: evaluar las fuentes de financiamiento, métodos de reclutamiento, redes comunicacionales, lugares de almacenamiento y otros recursos, con el fin de descubrir posibles puntos vulnerables.

La protección de las fronteras es una tarea crítica en cualquier plan de seguridad nacional. Los países Latinoamericanos comparten miles de kilómetros de fronteras ingresando a los distintos países millones de personas de las cuales la mayoría no poseen ciudadanía del país que visitan.

La seguridad de las fronteras exige la colaboración de varios organismos nacionales que apoyan al objetivo de seguridad de la nación: seguridad de transporte, control de inmigración, patrulla fronteriza, aduanas y seguridad marítima.

La capacidad para investigar y compartir información entre estos organismos es esencial para el cumplimiento de esa misión.

La solución



Sirtech®, VisuaLinks® y Digital Information Gateway (DIG™) son herramientas ideales para explorar diversas fuentes de datos y extraer, analizar y exponer en forma visual distintos patrones de actividad.

Con esta solución es posible:

- **Compartir información:** cada agente puede tener información de distintas fuentes, en una sola búsqueda.
- **Visualizar Datos Masivos:** exponer esquemas observando y analizando miles de registros.
- **Resumir:** Producir en forma rápida conteos de frecuencias e información estadística.
- **Rastrear y relacionar:** comparar valores de datos, (nombres, número de identidad y domicilios), con el fin de buscar y reconocer personas.
- **Identificar Rutas:** utilizar datos geográficos para ubicar y trazar rutas de entrada.



Tráfico de drogas

Las iniciativas de los organismos de seguridad buscan atacar a las organizaciones de tráfico de estupefacientes a través de esfuerzos coordinados a nivel local, provincial y nacional.

Los agentes de la ley deben adaptarse constantemente a nuevas situaciones, hacer mayores tareas de inteligencia, actualizarse tecnológicamente y ampliar la cooperación entre organismos para ser efectivos en sus esfuerzos.

Los organismos de seguridad de todos los niveles deben emplear métodos de análisis operativos (reactivos) y estratégicos (proactivos), apuntando a objetivos de corto y de largo plazo. Para realizar en forma efectiva ambos tipos de análisis, los agentes de seguridad deben poder acceder a un gran espectro de información, para descubrir vínculos ocultos entre casos que, normalmente, pasarían inadvertidos.

La solución

Sirtech®, VisuaLinks® y Digital Information Gateway (DIG™) están diseñados específicamente para recuperar información y formatos de fuentes diversas, mostrando así, esquemas de actividad y comportamiento ocultos.

Con esta solución es posible:

- **Compartir información:** Los agentes pueden acceder a información de varias fuentes.
- **Identificar Relaciones:** Revelar interacciones y conexiones entre delincuentes y organizaciones.
- **Visualizar datos masivos:** mostrar patrones, viendo y analizando grandes volúmenes de información, sin limitaciones de tamaño.
- **Descubrir patrones:** Graficar y analizar datos geográficos y cronológicos en forma rápida.
- **Resumir:** Producir rápidamente conteos de frecuencia e información estadística.
- **Rastrear y relacionar:** Comparar datos (nombres, documentos, domicilios), a fin de ubicar personas.

Vandalismo, hurto, violencia familiar, estafas con tarjetas de crédito, armamento ilegal, lavado de dinero, saqueo de domicilios, crímenes cibernéticos, robo de identidad y secuestros, son algunas de las actividades ilícitas que enfrentan a diario los organismos de seguridad.

¿Cuántos de estos delitos son cometidos por miembros de organizaciones?

Se cree que hasta el robo de autos es parte de un delito organizado, el cual genera miles de millones de dólares al año.

Uno de los desafíos, que presenta resolver toda clase de crímenes, es la búsqueda entre grandes cantidades de datos almacenados en distintos formatos y sistemas en todo el país, y de hecho en todo el mundo.

La capacidad para acceder y analizar la información a tiempo y correctamente es un factor imprescindible para identificar y hallar a los culpables. El Data mining es un enfoque que ayuda al análisis, localización de crímenes e inteligencia anti-criminal.



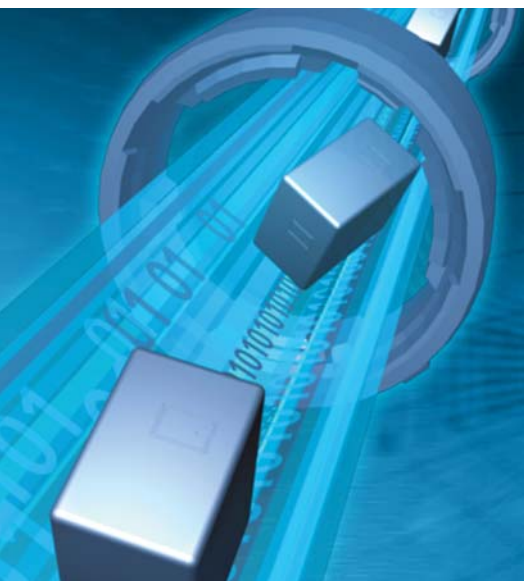
La solución



Sirtech®, VisualLinks® y Digital Information Gateway (DIG™) son herramientas ideales para recorrer grandes volúmenes de datos, extraer y analizar visualmente patrones de actividad.

Con esta solución es posible:

- Acceder a los Datos: Chequear toda la fuente de datos disponible en una sola búsqueda.
- Visualizar datos masivos: Trabajar con miles de registros de datos, sin límites de tamaño.
- Identificar Relaciones: Mostrar interacciones y relaciones entre todos los tipos de datos: grupos sospechosos, números de documento, vehículos, etc.
- Encontrar redes: Mostrar y analizar visualmente grupos de datos relacionados.
- Resumir datos: Generar rápidamente datos estadísticos.
- Rastrear y relacionar: Comparar valores, por ejemplo nombres de personas, usando Soundex y otros algoritmos.
- Compartir datos: Responder a consultas entre organismos.



Acceso a la información

Cualquier organismo de seguridad mantiene muchísimas fuentes de datos, desde bases de datos relacionales hasta sistemas de e-mail. Integrar estos datos en un formato estándar suele ser complejo, hasta imposible. Los sistemas de e-mail almacenan cientos de miles de mensajes y son inaccesibles para la mayor parte de las herramientas de extracción de datos, debido a la variedad de formatos que maneja (Exchange, Lotus Notes, UNIX, etc.).

Administrar la autenticación y el acceso a la información almacenada en distintas fuentes de datos puede ser una tarea ardua si no se cuenta con herramientas adecuadas.

Proporcionar el nivel de acceso adecuado sin comprometer la seguridad es un factor crítico en la elección de una herramienta.



La solución

Sirtech®, VisualLinks® y Digital Information Gateway (DIG™) están concebidos para extraer información de numerosas y variadas fuentes de datos, mediante una única búsqueda.

Con esta solución es posible:

- Revisar Datos Masivos: Extraer información relevante a partir de grandes volúmenes de e-mails acumulados (muchos millones)
- Extraer Datos: Emplear operadores de búsqueda en lenguaje estándar, y operadores complejos en lenguaje natural para buscar campos en las bases de datos.
- Búsquedas automáticas: Definir intervalos para disparar búsquedas automáticas de nueva información.
- Asegurar los datos: Un asistente lo ayuda a crear usuarios, grupos y seguridad de acceso.

Los delincuentes hacen legítimo el dinero obtenido en la actividad criminal - desde tráfico de drogas hasta evasión impositiva - mediante procesos de lavado de dinero.

Aunque la cantidad exacta de dinero que se lava anualmente aún se desconoce, los expertos estiman que son miles de millones de dólares - quizá hasta unos 100.000 millones.

Los que lavan dinero emplean varias capas de actividades para complicar la detección, investigación y enjuiciamiento de sus actividades. A menudo hacen esto estructurando transacciones, creando empresas para manipular cuentas, o bien presionando personas para que ignoren las leyes que obligan a informar operaciones.



La solución



Sirtech®, SYSTECH VIGIA®, VisualLinks® y Digital Information Gateway (DIG™) son imprescindibles para resaltar y ubicar transacciones sospechosas, que puedan revelar acciones financieras ilegales.

Con esta solución es posible:

- Acceder a los datos: Buscar y recuperar información de varias fuentes a la vez.
- Visualizar datos masivos: Revisar miles de transacciones financieras en busca de conductas extrañas y esquemas poco comunes.
- Mostrar estructuras: Identificar y mostrar relaciones entre personas y organizaciones implicadas en actividades criminales. Revisar cuentas: Revelar asociaciones entre cuentas y personas, bancos, organismos y otras cuentas.
- Identificar duplicados: Mostrar relaciones indirectas que presentan domicilios, cuentas o documentos con varios titulares.
- Analizar Transacciones: Presentar las diversas transacciones que usan los criminales.
- Ubicar Intercambios: Encontrar apropiaciones de fondos utilizando datos geográficos y cronológicos.



Análisis de llamadas telefónicas

El análisis de llamadas telefónicas es poco aprovechado en las investigaciones, dado el volumen de los datos a procesar.

Cuando se lleva a cabo adecuadamente el análisis de la actividad telefónica, puede por sí mismo, mostrar un conjunto de actividades fraudulentas, desde estafas con llamadas de larga distancia y teléfonos celulares, hasta esquemas de tráfico de drogas; además, puede confirmar relaciones entre personas y organizaciones.

Con las tecnologías de Data Mining los investigadores pueden descubrir vínculos entre números de teléfonos y personas u organizaciones, mostrando complejas redes de comunicación, ubicando objetos de investigaciones y rastreando esquemas secuenciales o cíclicos.

La solución

Sirtech®, VisualLinks® y Digital Information Gateway (DIG™) están perfectamente adecuados para identificar esquemas sospechosos de actividad telefónica.

Con esta solución es posible:

- Mostrar actividad intensa: Conexiones entre teléfonos, características comunes, rutas y redes entre grupos de números.
- Contar frecuencias: Resumir el volumen de llamadas desde y hacia ciertos números.
- Graficar actividad telefónica: Aplicar técnicas de trazado para revelar visualmente diversos patrones.
- Agrupar números: Dar un nombre a los números, y ver a un grupo, área o llamada como un solo elemento.
- Analizar Relaciones: Mostrar redes y relaciones que se hallan en crecimiento.

Las empresas de salud son candidatos ideales para las herramientas de análisis y visualización de datos, las cuales, pueden ser aplicadas de múltiples formas.

El acceso y análisis de datos relacionados, tanto con enfermedades y lesiones como con frecuencia y diagnóstico, ayudan a lograr un seguimiento preciso, asimismo, prever y enfrentar epidemias.

El análisis de patrones puede ayudar a la comunidad médica a prepararse para eventos frecuentes.

El análisis cuidadoso de los datos puede ayudar a descubrir fraudes en los que esté implicado un agente médico. Por intermedio del mismo podemos detectar situaciones tales como, unbundling, upcoding, fraude farmacéutico y pacientes fantasmas.



La solución

Sirtech®, VisuaLinks® y Digital Information Gateway (DIG™) son herramientas de avanzada para el análisis y la visualización de datos, capaz de manejar, analizar y presentar visualmente grandes volúmenes de datos.

Con esta solución es posible:

- Visualizar Datos Masivos – trabajar con miles de registros, sin limitaciones de tamaño.
- Identificar relaciones – mostrar interacciones y relaciones entre todos los datos: diagnósticos, áreas geográficas, síntomas, etc.
- Hallar redes – mostrar y analizar visualmente grupos de datos relacionados.
- Resumir datos – Generar información estadística en forma rápida.



Empresas farmacéuticas

Las empresas farmacéuticas tienen grandes bibliotecas con datos, los cuales, pueden ayudar al desarrollo de nuevas drogas rentables. El flujo de datos automatizados, proveniente de las investigaciones genéticas, es enorme. Otro resultado de la automatización es el desborde de datos sobre compuestos químicos, tales como estructura, atributos físicos y químicos.

Con la síntesis y seguimiento automatizados de compuestos, las empresas generan grandes bibliotecas con todas las posibles combinaciones, por lo que el número de compuestos puede alcanzar cientos de miles, incluso millones.

Muchas empresas farmacéuticas han invertido en tecnologías de data mining para que sus compuestos lleguen al mercado antes que los de la competencia.

La solución

Sirtech®, VisuaLinks® y Digital Information Gateway (DIG™) son herramientas adecuadas para recuperar y analizar datos de bases de recursos propias, de la industria y del gobierno, en forma rápida y concurrente.

Con esta solución es posible:

- Aislar el problema: Identificar secuencias genéticas adecuadas para el desarrollo de drogas.
- Curar la Cura: Analizar efectos colaterales.
- Identificar tendencias: Caracterizar en forma visual las recomendaciones y prescripciones médicas.
- Descubrir productos base: Buscar en grandes volúmenes de datos para mostrar clases de compuestos biológicamente activos.
- Dar un paso adelante: Examinar compuestos con actividad conocida, para revelar posibles esquemas de acción sobre estructuras aún no estudiadas.

Los fraudes le cuestan a las aseguradoras millones de dólares al año. Según el seguro, desde tenedores de pólizas hasta médicos y abogados han aparecido implicados en algún tipo de fraude con seguros. Los grupos especializados apuntan a las aseguradoras, y las atacan con miles de demandas fraudulentas cada año. Investigar este cúmulo de demandas dudosas es una tarea lenta y pesada que suele consumir muchos recursos. El manejo y análisis de datos puede evitar gran parte de los fraudes básicos; las aseguradoras pueden también automatizar las advertencias anticipadas ante posibles conductas fraudulentas, analizando y calificando a los tenedores de pólizas.



La solución



Sirtech®, SYSTECH VIGIA®, VisuLinks® and Digital Information Gateway (DIG™) son herramientas perfectas para identificar actividades sospechosas repetidas en distintas personas y empresas.

Con esta solución es posible:

- Establecer conexiones – mostrar relaciones entre distintos clientes de seguros.
- Mostrar relaciones indirectas – exhibir en forma visual relaciones que abarcan individuos y organizaciones que preparan fraudes.
- Encontrar identificaciones falsas – comparar nombres y valores, explorando los datos en búsquedas poco frecuentes.
- Rastrear y relacionar – Identificar nuevos objetivos y mostrar patrones, en cualquier base de datos.

Empresas



Cada año, las empresas y el gobierno pierden miles de millones de dólares por fraudes, derroche y mal uso de recursos.

Todas las empresas, grandes o pequeñas, pueden beneficiarse rastreando y analizando la web, e-mails, tráfico telefónico, acceso a recursos, órdenes de compra y otras actividades contables y administrativas; deben también observar cuidadosamente las transacciones que puedan dar lugar a fraudes, como pago de cuentas y devolución de mercaderías.

Además, las empresas necesitan analizar los procesos en forma proactiva para asegurarse de contar y aplicar los mejores métodos para ello.



La solución

Sirtech®, VisuLinks® y Digital Information Gateway (DIG™) son herramientas de última generación que permiten identificar actividades que resultan costosas y no suelen verse reflejadas en las auditorías tradicionales.

Con esta solución es posible:

- Analizar Procesos: Mostrar problemas sistémicos u operacionales de la empresa.
- Examine Statements: Identificar visualmente cheques o depósitos no reflejados mediante una conciliación.
- Identificar Fraudes: Mostrar transacciones dudosas, prácticas y fraude sistemático en diversas actividades.
- Inspeccionar las transacciones de venta: Mostrar elementos comunes entre terminales de venta y empleados del área, para productos utilizados en compras fraudulentas.
- Mostrar créditos o descubiertos excesivos: Mostrar los descubiertos excesivos, en los que los pagos pueden desviarse para obtener un beneficio ilegítimo.