# Análisis Inteligente de Datos y Visualización aplicadas a la Investigación Criminal
# Intelligent Data Analysis and Visualization applied to Criminal Investigation *

Sebastián P. WAHLER[1,2], Diego C. MARTÍNEZ[3], and Martín L. LARREA[3]

[1] Departamento de Informática, Facultad de Ingeniería, Universidad Nacional de la Patagonia San Juan Bosco, Mitre 655, U9100, Trelew, ARGENTINA.
spwahler@ing.unp.edu.ar
http://www.ing.unp.edu.ar/dpto-informatica.html

[2] Departamento de Informática, Procuración General, Ministerio Público Fiscal, Poder Judicial de la Provincia del Chubut, Belgrano 521, U9102, Rawson, ARGENTINA.
swahler@juschubut.gov.ar
https://www.mpfchubut.gov.ar

[3] Departamento de Ciencias e Ingeniería de la Computación, Universidad Nacional del Sur, Av. Alem 1253, B8000CPB Bahía Blanca, ARGENTINA.
dcm@cs.uns.edu.ar, mll@cs.uns.edu.ar
https://cs.uns.edu.ar/

Cambiar título del PAPER

**Resumen** Se presenta un estudio de las técnicas y metodologías actuales de análisis inteligente de datos y visualización para la asistencia en la investigación criminal, a partir de los registros de actividades delictivas, sus autores y las relaciones de datos que puedan derivarse a partir de ellas. Es de especial interés la identificación de redes ilegales, tales como bandas delictivas o criminales para propender a una persecución penal inteligente.

**Keywords:** Investigación Criminal · Análisis Inteligente de Datos · Redes Sociales · Visualización.

**Abstract** A study of the current techniques and methodologies of intelligent data analysis and visualization for assistance in criminal investigation is presented, based on the records of criminal activities, their authors and the data relationships that can be derived from them. The identification of illegal networks, such as criminal gangs, is of special interest in order to promote intelligent criminal prosecution.

**Keywords:** Criminal Investigation · Data Analysis · Social Networks · Visualization.

* Universidad Nacional de la Patagonia San Juan Bosco - Chubut - Argentina. Universidad Nacional del Sur - Bahía Blanca - Argentina.

## 1. Introducción

En la actualidad las actividades criminales habituales en una ciudad o región van desde hurtos y robos de poca importancia, hasta otros de mayor gravedad como amenazas, cibercrimen, abusos sexuales y homicidios. Todos ellos son registrados de diferentes formas por las fuerzas de la ley, con datos de variada precisión que incluyen usualmente la tipificación del delito, los datos en tiempo y espacio, y en muchas ocasiones los autores correspondientes.

Toda esta información respalda los procesos de investigación judicial de cada caso, pero con el transcurso del tiempo constituyen una extensa base de conocimiento sobre la cual es posible extraer valiosa información para la prevención del delito y la búsqueda de la justicia. Por ejemplo, es posible identificar relaciones entre personas de acuerdo a un análisis transitivo de eventos criminales en tiempo y espacio que sugieren la conformación de bandas delictivas. Las relaciones de amistad o conveniencia entre diversos autores de actividades criminales también puede inferirse de los registros delictivos y es de extrema relevancia para la prevención del delito y la resolución de casos inconclusos.

En este trabajo es de especial interés la aplicación de estas técnicas y tecnologías utilizando los registros de actividades criminales de la Provincia de Chubut a través de la colaboración del Ministerio Público Fiscal de la provincia (parte del Poder Judicial con autonomía funcional para la investigación y persecución de conductas delictivas) y las instituciones que lo asisten.

### 1.1. Antecedentes

Las organizaciones criminales son grupos que operan fuera de la ley, realizando actividades ilegales en beneficio propio y en detrimento de otros individuos o grupos sociales [1]. Pueden ser de diverso tamaño y cubrir áreas geográficas variadas, en muchos casos en conflicto con otras organizaciones similares. Una de las características particulares de este tipo de organizaciones es que, al estar enfocadas en actividades ilegales perseguidas por los organismos de seguridad pública, el anonimato y/o la discreción de sus miembros es de vital importancia. Esto requiere estudios de la información existente con el fin de identificar los criminales y realizar acciones apropiadas para la prevención del delito.

Los miembros de las organizaciones criminales tienen a su vez diversos grados de compromiso con cada una de ellas. En muchos casos los hechos criminales que son evidentes en la sociedad ocurren por individuos de baja jerarquía y responsabilidad en el grupo, motivados por la recompensa inmediata, las aspiraciones de ascenso y la reputación en su propio círculo de contactos. Asimismo, existen otros individuos de mayor jerarquía y responsabilidad en la organización criminal, que ostentan cualidades de liderazgo, intereses a largo plazo, y la constante preocupación por la conservación del poder para el beneficio personal y de la organización. Con frecuencia, son los individuos del primer grupo los que cometen delitos percibidos y registrados por las fuerzas policiales, mientras que los miembros del segundo grupo se mantienen con mayor discreción. Adicionalmente, las estructuras jerárquicas, la forma de operar, y la cultura inherente

de sus realidades socio-económicas imponen códigos propios que hacen difícil la identificación de la organización delictiva como un todo, con sus miembros y actividades relacionadas. Es aquí donde nuestro trabajo puede aportar un rol significativo.

## 2. Análisis de Redes Sociales (SNA)

Desde hace algunos pocos años, el Análisis de Redes Sociales (o SNA por sus siglas en inglés de Social Network Analysis) ha contribuido a las investigaciones criminales y a las actividades de inteligencia relacionadas.

Una red social modela individuos como nodos, vinculados entre sí por arcos o aristas que representan las relaciones entre esos individuos. El estudio de estas redes es importante porque se enfoca en la abstracción de las relaciones humanas sobre uno o más aspectos particulares [2] [3]. De esta manera, las redes conforman estructuras de grafos en las cuales es posible identificar diversas propiedades, tales como la relevancia o la importancia relativa de los nodos individuales en función de las conexiones existentes o el flujo de información. De acuerdo a Sage [4] , existen cuatro pilares fundamentales del análisis de redes: el reconocimiento de la importancia de las relaciones sociales entre los individuos, la recolección y análisis de datos sobre estas relaciones entre los individuos, la importancia de la representación visual de estos datos y la necesidad de modelos matemáticos y computacionales que expliquen los patrones de conexión entre los individuos.

En particular, la vinculación entre el estudio de las redes sociales y la investigación criminal ha sido encarada por varios autores. A mediados de los 70 se utilizaban modelos básicos para establecer y cualificar las relaciones entre individuos o actores de un escenario particular, definiendo grafos de acuerdo a la información recolectada [5], pero el procesamiento era mayoritariamente manual y con varias etapas de refinamiento y valoración de datos. Esta es la que según Klerk en [6] sería la primera generación de análisis de redes en criminalística. La segunda generación involucra el uso de herramientas computacionales que automatiza parte de la tarea de registro y estructuración de datos. Estas herramientas además aumentaron notoriamente la cantidad de datos que se pueden analizar, haciendo mucho más ágil su registro y consulta. La tercera y actual generación establece la definición de modelos y técnicas matemáticas para la generación de nuevo conocimiento, como la identificación de posiciones de poder e influencia o la calidad de potenciales testigos o informantes. Métricas como la centralidad de un nodo en un grafo son especialmente útiles en este escenario.

Uno de los trabajos más importantes al respecto es el de Krebs [7], en donde se identifica una parte de la red de terroristas que fué responsable de los atentados del 11 de septiembre de 2001 en Nueva York. Aquí identifica agrupaciones de individuos que se conectan entre sí por los pilotos responsables del secuestro de las aeronaves. Otros estudios similares han sido efectivos en consecuencia [8] [9] [10]. Por otro lado, el análisis de redes sociales ha cobrado también interés en la investigación criminal tradicional como las estructuras de la mafia o el nar-

cotráfico [11] [12] [13] [14] [15]. Estudios como el de Malm [16] han permitido identificar roles en la cadena de suministros para la fabricación de drogas ilícitas, lo que acarrea diferentes riesgos penales para cada uno de los colaboradores. Otros estudios se enfocan en el uso del análisis de las redes sociales para otras actividades criminales, como el tráfico ilícito de arte [17], el lavado de dinero [18] [19], corrupción policial [20] y bandas juveniles [21] [22]. Existen también líneas de investigación en la disciplina referente al cibercrimen [23] [24] [25]. Es claro entonces que el análisis de redes sociales puede ser aplicado a un amplio rango de actividades criminales y ha demostrado modelar apropiadamente características propias de las organizaciones ilegales, asistiendo a la prevención del delito y al diseño de políticas adecuadas para enfrentar estas actividades.

Existen sin embargo algunas dificultades que requieren aún estudios intensivos. La cantidad de información que debe manejarse es enorme, en muchos casos con información incompleta, contradictoria y no menos frecuentemente incorrecta. Además, las relaciones humanas tradicionales se mezclan naturalmente con las interacciones ilícitas entre los individuos por lo que es necesario identificar apropiadamente su naturaleza y consecuencias y determinar los límites sensatos de la red social analizada.

Actualmente los organismos estatales encargados de la Justicia y la prevención del delito cuentan con registros informatizados de las actividades criminales detectadas, así como de las etapas y eventos del subsecuente proceso penal. En particular, para este trabajo es de especial interés la información producida a tal efecto por las fuerzas policiales de la Provincia del Chubut y su Poder Judicial de la mano del Ministerio Público Fiscal (MPF). Existen decenas de miles de registros que son utilizados principalmente para la acción penal, pero que pueden ser empleados para modelar diferentes redes sociales sobre las cuales aplicar un análisis matemático y computacional en la búsqueda de nueva información. Esto permitirá conocer más sobre las actividades criminales y sus autores en la jurisdicción de esa provincia, con las particularidades propias de la información registrada digitalmente.

El análisis y exploración de estos grandes conjuntos de datos y sus relaciones debe ser asistido por técnicas y herramientas que faciliten este proceso y reduzcan la carga cognitiva que recae sobre los usuarios. En tal sentido, el área de Visualización de Información, en particular la Visualización de Grandes Conjuntos de Datos, busca asistir a los usuarios de tal manera. La aplicación de técnicas visuales para la representación de este tipo de información no es nueva [26] [27] [28]. También es importante el estudio de las tareas e interacciones que la visualización debe soportar [29], ya que son estas interacciones las que facilitan la exploración de la visualización de información.

## 3. Marco de Trabajo - Ministerio Público Fiscal del Chubut

En el marco de trabajo se ha optado por investigar en base al análisis criminal de redes delictivas en el Ministerio Público Fiscal del Chubut [30], perteneciente al Poder Judicial de la provincia.

Coirón, es el sistema informático que colabora con la administración del flujo de casos ingresados al Ministerio Público Fiscal del Chubut.

Es una herramienta que permite registrar, comunicar y gestionar las actividades, trámites y actuaciones que se realizan para un caso penal, desde la denuncia hasta su finalización.

Como herramienta de registro construye una base de datos con el historial de cada caso, así como de las personas involucradas y de los responsables de la gestión en cada oficina. Como herramienta de comunicación, agrupa la información, entrecruza las relaciones, identifica pertenencias y vinculaciones entre casos, personas, sus antecedentes y sus lazos.

Como herramienta de gestión administra el flujo de casos y el trabajo de los integrantes de las oficinas responsables de los mismos. Permite planificar, organizar, coordinar y controlar el flujo de trabajo afín a cada caso y la sumatoria de ellos. Ha sido desarrollado a medida de las necesidades del Ministerio Público Fiscal del Chubut, tomando como base el Código Procesal Penal vigente en el Chubut y adaptado a los lineamientos estratégicos de diseño y gestión de Oficinas Fiscales definidos por la Procuración General.

Su progreso, mantenimiento y mejora continua está a cargo de un Equipo de Desarrollo del Departamento de Informática del Área de Planificación y Control de Gestión de la Procuración General.

Una vez registrada toda la información relacionada a un hecho, y con ayuda de herramientas y vinculaciones con otros sistemas, se pueden obtener salidas que permiten llevar adelante la investigación de un caso o de un conjunto de hechos con características comunes.

Actualmente nos encontramos trabajando en la incorporación de herramientas de visualización de información que permitirán ver en modo gráfico lo que hoy se muestra en grillas, y listados, potenciando el análisis que realizarán luego los especialistas.

Un medio de enfrentar, "a través del análisis criminal, la persecución penal de sujetos prolíficos es el perfilamiento relacional entre ellos, a través de la realización de vinculación de compañeros de delitos y de redes sociales; a fin de identificar si forman parte de una banda o alguna organización criminal mayor o de un fenómeno delictual más extenso" [31].

Los analistas de redes sociales utilizan dos tipos de herramientas matemáticas para representar información sobre los patrones de relaciones entre actores sociales: matrices y grafos. Estos últimos son de gran ayuda visual cuando se trabaja con una gran cantidad de registros.

Existen muchas variaciones en los grafos, pero todos ellos comparten la característica común del uso de un círculo etiquetado para cada actor en la población

que describimos y segmentos de línea entre pares de actores para representar el hecho que existe un vínculo entre ellos.

Se denomina "Grupo de Pertenencia" en el Sistema Coirón a la relación directa que existe entre un individuo dentro del universo de personas cargadas como actores de delitos (roles: denunciado, sospechoso o imputado) y otros individuos del mismo universo, con los cuales existan uno o más casos penales en común.

Crear un módulo de software "Red de Grupos de Pertenencia" donde se muestre gráficamente las relaciones entre las personas involucradas en los casos penales es el objetivo principal de esta investigación. No sólo enfocarse en el grupo de pertenencia de una persona en particular, sino que mediante una visualización y con diversos filtros de búsqueda se logre mostrar gráficamente las relaciones entre un determinado grupo de personas y de esta manera poder inferir la conformación de posibles bandas delictivas.

La idea central es reflejar de manera gráfica, mediante un Grafo, los grupos de pertenencia. Dentro del mismo se le llamará nodo a cada círculo, y representa a una persona (con los roles ya mencionados: imputado, sospechoso o denunciado) involucrada en dos o más casos penales. Existe un gran cúmulo de personas en el sistema con sólo un caso con rol de denunciado, por esa razón se los excluye del universo a analizar, no obstante podrían ser parte del dataset a visualizar si alguno/s de ellos se encuentran relacionados con otros nodos del primer grupo. El tamaño del nodo posee una relación directa con la cantidad de casos penales en los que se encuentre involucrada la persona. Cuanto mayor sea el tamaño del nodo en más cantidad de casos penales estará involucrado.

Los segmentos de líneas entre pares de nodos, vinculan a las personas entre sí y representan el o los casos que tienen en común. El grosor de la vinculación será directamente proporcional a la cantidad de casos en común entre un par de personas.

Hay nodos que se encontrarán aislados en el grafo, esto no significa que no estén involucrados en casos, sino que quizás no existan relaciones para el filtro de búsqueda que se utilice en esa vista en particular.

Supongamos que una persona "A" se encuentra asociada a 8 casos penales, una persona "B" a 4 y una persona "C" a 2 casos. Agreguemos que las personas "A" y "B" se encuentran relacionadas entre sí, por estar en 3 casos en común (casos 1, 2 y 3). Por otro lado las personas "A" y "C" también se encuentran relacionadas, por tener un caso en común (caso 4). Una representación gráfica de dicha situación se muestra a continuación en la Figura 1, y puede observarse el doble de tamaño entre el nodo "A" y el nodo "B", representando justamente la diferencia de casos entre ambos nodos (8 y 4 casos). También se ve a simple vista el grosor del enlace entre "A" y "B" tres veces más grande que el enlace entre "A" y "C" (3 casos en común entre el primer par de nodos, y sólo un caso para el último par de nodos mencionado).

Explicar ejemplos del grafo

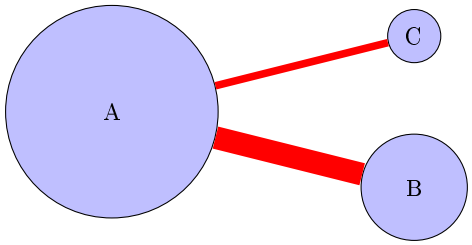


**Figura 1.** Ejemplo de relación entre tres personas.

## 4. Descripción general de los Datos

En esta sección, describimos nuestro conjunto de datos de casos penales y la red de personas asociada, así como algunas características interesantes que se han de mencionar.

**Dataset de Delitos** Nuestro conjunto de datos consta de casos penales, actuaciones (bitácora de eventos del proceso penal), delitos, personas, elementos (denunciados y secuestrados), todos ellos relacionados; entre octubre de 2006 y mayo de 2022 en la Circunscripción Judicial de Trelew - Chubut. Este conjunto de datos incluye lugares (relativos a personas y a hechos delictivos), fechas, estados procesales de los casos y las personas, como así también los vínculos entre todos los conjuntos mencionados. En el Cuadro 1, resumimos algunas de las características importantes del conjunto de datos.

Tengo que hacer un restore de la DB de trelew en una fecha en particular, y armar un script de SQL para generar una tabla de resumen (cantidad de casos totales, personas, delitos, etc) para completar la info

**Cuadro 1.** Totalizadores de tablas generales en la base de datos utilizada

| Característica | Cantidad total |
|---|---|
| Casos | 105586 |
| Personas | 132950 |
| Personas en Casos | 183348 |
| Delitos | 113010 |

**Propiedades de la red** A partir de los datos de los casos penales, pudimos construir la red de Grupos de Pertenencia. En esta red, se eliminan los nodos de aquellas personas cuyos roles no sean referidos a actores delictivos, como ser: denunciantes, víctimas, damnificados, etc. En la Figura 2 se muestra una visualización de la red. En la misma se puede observar un grafo compuesto de las 200 personas con más Casos Penales registrados en el Sistema de Gestión Coirón (con los siguientes criterios: involucradas en al menos un caso con rol de imputado, sospechoso o denunciado; se incluyen personas fallecidas, menores y

personas jurídicas). Se visualizan además en la figura todas las relaciones que existen entre esas 200 personas y sus grupos de pertenencia.

También hemos incluido estadísticas resumidas en el Cuadro 2, en donde se pueden ver la cantidad de nodos y vértices totales con los que cuenta el dataset utilizado, como así también otros parámetros interesantes de analizar para el estudio de redes sociales.

Al analizar la composición de la red obtenida podemos observar las relaciones que existen entre los nodos y como se "equilibra" el grafo, haciendo que aquellos nodos con pocas o nulas relaciones queden en la periferia de la gráfica. Sumado a ello también es apreciable la medida de centralidad de aquellos nodos que son rodeados por sus relacionados.

Una aproximación más clara para denotar la medida de centralidad puede verse reflejada en la Figura 3, en donde se visualiza sólo las 10 personas con más Casos y sus grupos de pertenencia. Claramente esos 10 nodos principales quedan rodeados de sus grupos de pertenencia y se pueden observar transitividades entre ellos a través de nodos que conforman parte del grupo de pertenencia de más de un nodo principal.

hablar un poco de la distribución de datos

script de SQL para generar la tabla 2(cantidad de nodos, vertices, ver si puedo calcular transitividad, y otros parámetros

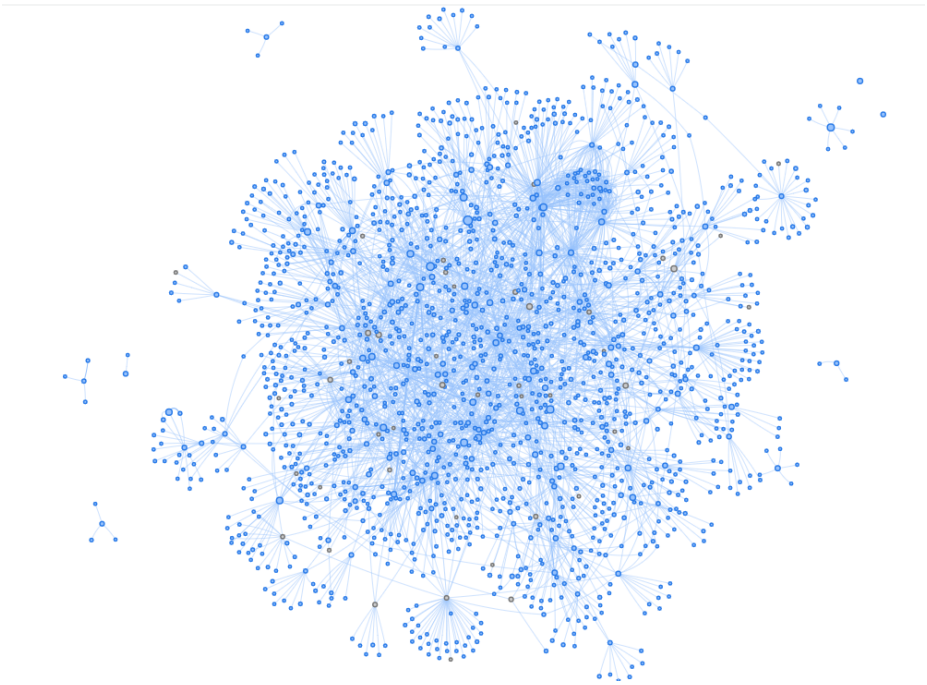

**Figura 2.** Grafo obtenido del Sistema Coirón. 200 personas con más casos y sus relaciones (con los siguientes criterios: involucradas en al menos un caso con rol de imputado, sospechoso o denunciado; se incluyen personas fallecidas, menores y personas jurídicas)

**Cuadro 2.** Resumen del conjunto de datos utilizado.

| **Característica** | **Cantidad total** |
|---|---|
| Nodos | 33178 |
| Enlaces | 16964 |
| Relaciones Nodos/Enlaces | 60513 |

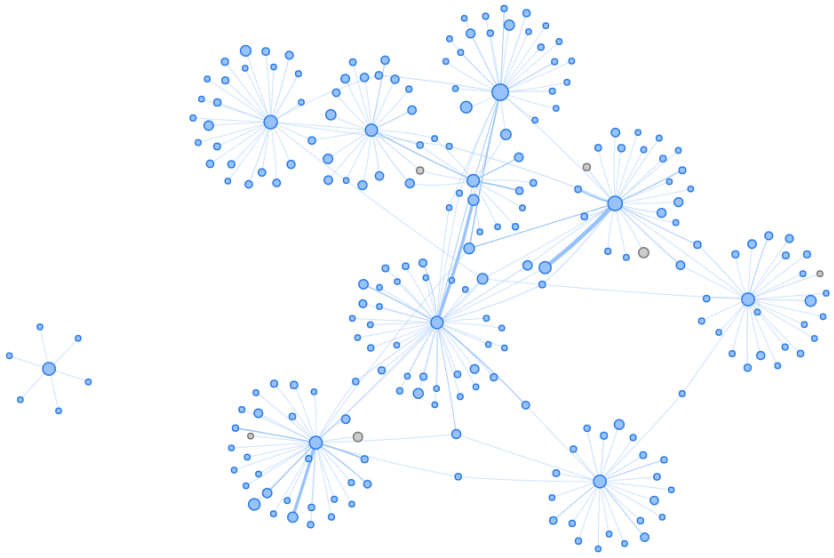

**Figura 3.** 10 personas con más casos en Coirón, con sus relaciones

**Centralidad de Grado** La centralidad de grado es una de las medidas más simples de centralidad. En esta se mide el número de enlaces o conexiones que tiene un nodo con los demás nodos pertenecientes a un grafo. Cuando se aplica un análisis de este tipo pueden determinarse diferentes medidas. Por ejemplo, en redes sociales podemos medir el grado de entrada de un nodo como la popularidad o preferencia que posea y la salida definirla como un indicador de sociabilidad. En nuestro caso de estudio, los miembros de las bandas delictivas modifican dinámicamente sus relaciones con otros miembros de la red, lo que resulta en un cambio de su rol e importancia. Una serie de medidas de centralidad de grado pueden ayudar a identificar estos cambios. Estas estadísticas se pueden utilizar para filtrar la vista de la red en función del valor de un nodo específico y resaltar su posición dentro de la red. El grado de centralidad en nuestro grafo se definirá entonces como el número de enlaces directos que tiene un delincuente. Un nodo con un alto grado puede verse como un "centro", un nodo activo e importante en la red [32].

**Transitividad** El coeficiente de agrupamiento (transitividad) de un gráfico mide el grado de conexión de una red. Altos coeficientes de agrupamiento significan la presencia de un alto número de triángulos en la red. Es bien conocido en la biblografía [34] que las redes sociales muestran valores altos del coeficiente de agrupamiento cuando reflejan la estructura social subyacente de los contactos entre amigos/conocidos. Además, los valores altos del coeficiente de agrupamiento local se consideran un indicador confiable de los nodos cuyos vecinos están muy bien conectados y entre los cuales puede fluir una cantidad sustancial de información.

hablar de vis.js, quizás agregar algo de código

**Desarrollo de la Visualización**

Para llevar a cabo la visualización del conjunto de datos obtenidos del análisis inteligente anteriormente descripto, se utilizó Vis.js [35], una biblioteca o librería de visualización dinámica basada en lenguaje Javascript. La misma está diseñada para que sea fácil de usar, para manejar grandes cantidades de datos dinámicos y para permitir la manipulación y la interacción con los datos. La biblioteca consta de los componentes DataSet, Timeline, Network, Graph2d y Graph3d.

En nuestro caso particular utilizamos el componente "Network", que permite mostrar redes en grafos. La visualización es fácil de usar y admite formas, estilos, colores, tamaños, imágenes, etc. Funciona sin problemas en cualquier navegador moderno para hasta unos pocos miles de nodos y bordes. Para manejar una mayor cantidad de nodos, Network tiene soporte de agrupamiento. La red utiliza canvas HTML para la renderización.

Vis.js proporciona implementaciones de algoritmos de diseño forzados "Force-directed graph drawing". Estos algoritmos dirigidos por fuerza intentan posicionar los nodos considerando las fuerzas entre dos nodos (atractivos si están conectados, repulsivos de lo contrario). Generalmente son iterativos y mueven los nodos uno por uno hasta que ya no es posible mejorar o se alcanza el número máximo de iteraciones. Los enlaces tienen más o menos la misma longitud y el

menor número posible de enlaces cruzados. Los nodos conectados se juntan más mientras que los nodos aislados se alejan hacia los lados.

Agrego ejemplos de código y más comentarios técnicos sobre vis.js?

## 5. Identificación de posibles Bandas Delictivas

Descripción de identificación de bandas

En esta sección, describimos nuestro problema, algunos de los enfoques prácticos existentes utilizados por las fuerzas de la ley y nuestro enfoque basado en la teoría de grafos con características generadas principalmente por la distribución de los datos anteriormente descrita.

**Métodos existentes** Aquí describimos las técnicas comunes que las fuerzas de seguridad suelen utilizar para predecir posibles bandas delictivas.

Las personas nos movemos habitualmente entre lugares conocidos o nodos (hogar, trabajo, supermercado, restaurante) y por las mismas calles o rutas. La teoría sugiere que cuando ocurre un delito es porque se cruzan delincuentes y víctimas dentro de algunas de estas zonas de actividad (nodo, ruta). A partir del análisis del lugar del delito se pueden determinar distintos tipos de víctimas y delincuentes que lo frecuentan, entender por qué concurren a ese lugar y qué hace que se encuentre la dupla delincuente-víctima. Es una manera estructurada de conocer e investigar patrones de comportamiento.

Por otro lado se puede deducir que los delincuentes se comportan igual que el resto de las personas, realizan actividades diariamente, se mueven por rutas conocidas para ir de la casa al trabajo, o a algún otro lugar que frecuenten. Es decir, mantienen una cierta rutina en sus vidas. Un delincuente tenderá a cometer un delito en algún lugar que se encuentre dentro o cerca del recorrido que realiza diariamente para trasladarse desde la casa al trabajo, del trabajo a algún lugar de recreación u otro lugar habitual.

De ambos enfoques se busca encontrar la mayor cantidad de patrones de ocurrencia entre diversos hechos de similar criminalidad y patrones horarios, como así también las zonas geográficas en donde se producen.

La naturaleza de los vínculos de los integrantes de una banda delictiva es una variable que aporta información sobre las características y similitudes de los miembros del grupo, atendiendo a criterios concretos: vínculo familiar, cultural, de proximidad (provienen del mismo barrio), han compartido prisión, de especialización (habilidades delictivas), la experiencia u otras capacidades, y otros tipos de vínculo.

**Enfoque propio** Ante los enfoques teóricos y prácticos estudiados anteriormente, nuestro desarrollo de software propio, que permite mostrar de manera gráfica las relaciones entre actores delictuales en el Sistema Penal de la Provincia del Chubut, se potencia como una herramienta vital de apoyo en la toma de decisiones de la investigación penal de bandas delictivas.

Poder visualizar relaciones entre las personas involucradas en casos penales ayuda a los especialistas a detectar triangulaciones, transitividades y por supuesto centralidades en la Red. Todo ello, sumado a los indicios de investigación

y la propia expertís en la temática completan una herramienta de análisis para determinar ciertas bandas o grupos altamente relacionados.

En el año 2019 existieron investigaciones vinculadas a reiterados robos de televisores LCD en domicilios, como así también una serie de hechos consecutivos vinculados al robo de cajas fuertes en empresas del parque industrial de la ciudad de Trelew.

La UAC (Unidad de Análisis Criminal), organismo auxiliar de la Procuración General perteneciente al Ministerio Público Fiscal del Chubut, sirvió como equipo de apoyo en la investigación de ambos modus operandi, haciendo uso de toda la información de los legajos fiscales, consultas generales y específicas contenidas en el Sistema Coirón. Fue de vital uso la información referida a los grupos de pertenencia de cada persona, pero devino en un arduo trabajo entrecruzando información de personas, para dar con las supuestas bandas delictivas detrás de estos hechos.

Dichas investigaciones sirvieron como puntapié inicial para realizar esta investigación y poder facilitar la información ya contenida en el sistema de gestión penal, de otra manera, de una forma más directa y visual a la hora de investigar, que sirva directamente como apoyo a la toma de decisiones en las investigaciones de bandas delictivas.

## 6. Trabajos futuros

trabajos futuros - más descripción además de lo teórico

**Estudio de Centralidad de Intermediación (Betweenness centrality)** Obtiene la medida en que un nodo en particular se encuentra entre otros nodos en una red. Estos elementos intermedios pueden ejercer control estratégico e influencia sobre muchos otros. El problema central de esta medida de centralidad es que un actor es central si se encuentra a lo largo de los caminos más cortos que conectan otros pares de nodos. Un individuo con una alta intermediación puede ser quien dirige la red. Un delincuente de este tipo es muy buscado, ya que su aprensión puede desestabilizar una red criminal o incluso hacer que se destruya [32].

**Estudio de Centralidad de Cercanía (Closeness centrality)** Es la inversa de la suma de los caminos más cortos (geodésicas) que conectan un nodo particular con todos los demás nodos de una red. La idea es que un delincuente es central si puede interactuar rápidamente con todos los demás, no solo con sus primeros vecinos [33]. En el contexto de las bandas delictivas, esta medida destaca aquellos actores con la distancia mínima entre sí, lo que les permite comunicarse más rápidamente que cualquier otra persona en la organización. Por esta razón, la adopción de la centralidad de cercanía es crucial para poner en evidencia dentro de la red a aquellos individuos que están más "cerca" de otros (en términos de datos en común en los Casos en los que se encuentran involucrados). Además, los valores altos de centralidad de cercanía en este tipo de

redes considerarse como un indicador de la "capacidad" del actor para difundir información rápidamente a todos los demás actores de la red.

**Estudio de Centralidad de Vector Propio o Autovector (Eigenvector centrality)** Es otra forma de asignar la centralidad a un actor de la red basada en la idea de que si un nodo tiene muchos vecinos centrales, también debería ser central. Esta medida establece que la importancia de un nodo está determinada por la importancia de sus vecinos. En el contexto de las redes de telecomunicaciones por ejemplo, la centralidad del vector propio generalmente se considera como la medida de influencia de un nodo dado. Altos valores de centralidad de vector propio son alcanzados por actores que están conectados con vecinos de alta puntuación, que a su vez, heredaron tal influencia de sus vecinos de alta puntuación y así sucesivamente. Esta medida refleja una característica importante en redes de comunicación, pero será interesante ver si se pueden extraer ciertas medidas dentro de nuestro campo de estudio.

**Estudio de herramienta de visualización "neovis.js"** Biblioteca de visualización de gráficos de JavaScript para crear visualizaciones que se pueden incrustar en una aplicación web, con la posibilidad de crear visualizaciones de datos gráficos que utilizan los resultados de algoritmos gráficos como Centralidad por PageRank y detección comunitaria. Dichas interacciones y configuraciones con los algoritmos, no son posibles de manipular con Vis.js.

## 7. Conclusiones

Descripción de conclusión

En el presente trabajo se presentó un estudio de las técnicas y metodologías actuales de análisis inteligente de datos y visualización para la asistencia en la investigación criminal. Todo ello a partir de los registros de actividades delictivas, sus autores y las relaciones de datos que pueden derivarse a partir de ellas. Fué de especial interés la identificación de redes ilegales, tales como bandas delictivas o criminales para propender a una persecución penal inteligente.

Pasar la bibliografía a un archivo aparte bib

## Referencias Bibliográficas

1. Finckenauer JO. Problems of definition: What is organized crime? Trends in Organized Crime. 2005; 8(3):63–83. https://doi.org/10.1007/s12117-005-1038-4
2. Krishna Raj P.M.Ankith MohanK.G. Srinivasa. Practical Social Network Analysis with Python. Springer, 2018. ISBN: 978-3-319-96746-2.
3. Burcher, Morgan. Social Network Analysis and Law Enforcement: Applications for Intelligence Analysis. Serie Crime Prevention and Security Management, 2020. ISBN 978-3-030-47770-7
4. L.C. Freeman, The SAGE handbook of social network analysis, eds. J. Scott, P.J. Carrington, SAGE Publications Ltd., 2011.
5. W.R. Harper, D.H. Harris, The application of link analysis to police intelligence. Hum. Factors 17(2), 157–164 (1975).

6. P. Klerks, The network paradigm applied to criminal organisations: theoretical nitpicking or relevant doctrine for investigators? Recent developments in the Netherlands. Connections 24(3), 53–65 (1999)
7. V. Krebs, Mapping networks of terrorist cells. Connections 24(3), 43–52 (2002)
8. R.M. Medina, Social network analysis: a case study of the Islamist terrorist network. Secur. J. 27(1), 97–121 (2014)
9. J. Qin, J.J. Xu, D. Hu, M. Sageman, H. Chen, Analyzing terrorist networks: a case study of the global jihad. Lect. Notes Comput. Sci. 3495, 287–304 (2005)
10. E. Stollenwerk, T. Dörfler, J. Schibberges, Taking a new perspective: mapping the Al Qaeda network through the eyes of the UN Security Council. Terror. Political Violence 28(5), 950–970 (2016)
11. M. Bouchard, J. Amirault, Advances in research on illicit networks. Glob. Crime 14(2–3), 119–122 (2013)
12. D.A. Bright, C. Greenhill, M. Reynolds, A. Ritter, C. Morselli, The use of actor-level attributes and centrality measures to identify key actors: a case study of an Australian drug trafficking network. J. Contemp. Crim. Justice 31(3), 262–278 (2015a)
13. L. Giommoni, A. Aziani, G. Berlusconi, How do illicit drugs move across countries? a network analysis of the heroin supply to Europe. J. Drug Issues 47(2), 217–240 (2016)
14. C. Morselli, Hells Angels in springtime. Trends Org. Crime 12(2), 145–158 (2009)
15. C. Morselli, Assessing vulnerable and strategic positions in a criminal network. J. Contemp. Crim. Justice 26(4), 382–392 (2010)
16. A. Malm, G. Bichler, Networks of collaborating criminals: assessing the structural vulnerability of drug markets. J. Res. Crime Delinq. 48(2), 271–297 (2011)
17. G. Bichler, A. Malm, Small arms, big guns: a dynamic model of illicit market opportunity. Glob. Crime 14(2–3), 261–286 (2013)
18. A.F. Colladon, E. Remondi, Using social network analysis to prevent money laundering. Expert Syst. Appl. 67, 49–58 (2017)
19. M.R.J. Soudijn, Using strangers for money: a discussion on money-launderers in organized crime. Trends Org. Crime 17(3), 199–217 (2014)
20. M. Lauchs, R. Keast, N. Yousefpour, Corrupt police networks: uncovering hidden relationship patterns, functions and roles. Polic. Soc. 21(1), 110–127 (2011)
21. J.M. McGloin, Policy and intervention considerations of a network analysis of street gangs. Criminol. Public Policy 4(3), 607–635 (2005)
22. G. Bichler, A. Malm, J. Enriquez, Magnetic facilities: identifying key juvenile convergence places with social network analysis. Crime Delinq. 60(7), 971–998 (2014)
23. D. Décary-Hétu, Information exchange paths in IRC hacking chat rooms, in Crime and networks, ed. by C. Morselli, (Routledge, New York, 2014)
24. D. Décary-Hétu, B. Dupont, The social network of hackers. Glob. Crime 13(3), 160–175 (2012)
25. D. Décary-Hétu, B. Dupont, Reputation in a dark network of online criminals. Glob. Crime 14(2–3), 175–196 (2013)
26. M1. Xu, Jennifer, and Hsinchun Chen. "Criminal network analysis and visualization." Communications of the ACM 48.6 (2005): 100-107.
27. M2. Feng, Mingchen, et al. "Big data analytics and mining for effective visualization and trends forecasting of crime data." IEEE Access 7 (2019): 106111-106123.
28. M3. Mathew, Ammu, et al. "Criminal Networks Mining and Visualization for Crime Investigation." Caniya and P, Mufeed and Raj, Asha, Criminal Networks Mining and Visualization for Crime Investigation (July 8, 2021) (2021).

29. M4. Chen, Hsinchun, et al. "Visualization in law enforcement." CHI'05 extended abstracts on Human factors in computing systems. 2005.
30. https://www.mpfchubut.gov.ar/
31. L. González, G. Rua. Sistemas Judiciales: Una perspectiva integral sobre la administración de justicia - Análisi Criminal, Publicación anual del CEJA e INECIP. N°23. Año 2019.
32. K. M. Carley, Destabilization of covert networks, Comput. Math. Organ. Theory 12 (1) (2006) 51-66.
33. M. Newman, A measure of betweenness centrality based on random walks, Social Networks 27 (1) (2005) 39-54.
34. S. Wasserman, K. Faust, Social network analysis: methods and applications, Cambridge University Press, 1994.
35. https://visjs.org/