Análisis comparativo de topologías y modularidad en dos redes humanas: una red clandestina y una red institucional*

Jessica Aquino, Pedro Cataño, Silvana Contreras, Christian Lombardo

Mayo 2025

Abstract

Este trabajo parte del interés por comparar redes humanas de contacto que responden a lógicas organizativas opuestas: una institucional y abierta, y otra clandestina y compartimentada. Para ello se seleccionaron dos grafos reales de comunicaciones: la red Email-EU (correos electrónicos entre empleados de una institución europea) y la red Terroristas (contactos entre involucrados en los atentados de Madrid de 2004). El objetivo es caracterizar sus topologías, detectar diferencias en la distribución de centralidades, analizar su robustez estructural y explorar sus comunidades. Se aplicaron métricas clásicas de teoría de grafos y se compararon ambas redes con prototipos. Los resultados muestran que ambas redes presentan propiedades de mundo pequeño, aunque con diferencias: Email-EU posee mayor dispersión de grados y robustez estructural, mientras que Terroristas es más densa y vulnerable a ataques dirigidos. El análisis de comunidades revela una modularidad alta en ambas, aunque con distinta segmentación. Concluimos que las exigencias funcionales —eficiencia en entornos institucionales y compartimentación en redes encubiertas— se reflejan en sus arquitecturas topológicas. La comparación con prototipos sugiere que ninguna red modelo logra capturar simultáneamente todas las propiedades observadas, lo que evidencia la complejidad estructural de las redes humanas reales.

1. Introducción

El análisis de redes complejas ha demostrado ser una herramienta poderosa para comprender fenómenos estructurales y dinámicos en sistemas sociales, tecnológicos y biológicos.

En este trabajo nos proponemos aplicar conceptos fundamentales de teoría de grafos al estudio de dos redes humanas reales de contacto: una red de correos electrónicos en una institución europea de investigación (Email-EU), y una red de vínculos entre individuos acusados de participar en los atentados de Madrid en 2004 (Terroristas). Ambas presentan estructuras diferenciadas en cuanto a tamaño, densidad y propiedades topológicas, lo que permite contrastar modelos de organización formal y clandestina.

La elección de estos datasets se basa en su potencial para explorar cómo diferentes objetivos funcionales (eficiencia comunicacional en un entorno laboral frente a compartimentación en una red ilegal) se reflejan en la arquitectura de los grafos. Para ello, se analizarán sus atributos de manera comparativa con prototipos de redes, sus centralidades, su robustez y la modularidad.

Diversos estudios han aplicado el análisis de redes sociales al estudio de organizaciones clandestinas, destacando su utilidad para comprender la estructura y las vulnerabilidades de estos sistemas (Zech,

*TP 1 de la materia **Data Mining en Ciencia y Tecnología**. Mayo 2025. Maestría en Explotación de Datos y Descubrimiento de Conocimiento. Facultad de Ciencias Exactas y Naturales. Universidad de Buenos Aires.

2016 y Diesner, 2005) (1; 4). Algunos autores han enfatizado las diferencias estructurales entre redes encubiertas y abiertas (Clark, 2016 y Campbell 2016)(2; 3), lo cual respalda la comparación desarrollada en este trabajo.

La aplicación de este enfoque a entornos organizacionales formales también ha sido documentada en estudios previos. Por ejemplo, Kumar y Gupta (2022) analizaron la red de correos electrónicos de una institución europea utilizando métricas clásicas de grafos, e identificaron propiedades de mundo pequeño y la existencia de nodos clave en la estructura comunicacional (5). Por su parte, Clarke y Preece (2019) abordaron el análisis de redes institucionales desde una perspectiva que combina el estudio estructural con consideraciones éticas sobre la trazabilidad de roles jerárquicos a partir de los patrones de interacción (6).

Estos antecedentes confirman el potencial del estudio de grafos para revelar dinámicas internas complejas en organizaciones humanas.

Nuestro análisis preliminar de estas propiedades topológicas revela patrones sobre los cuales se plantean las siguientes hipótesis: se espera que la red Terroristas presente una estructura de compartimentos rígidos, reflejada en un alto coeficiente de clustering y una modularidad fuerte, resultado de estrategias de compartimentación y seguridad operativa. En esta red será más relevante la centralidad de intermediación (puentes entre células). En contraste, en Email-EU, se anticipa una estructura más abierta, con múltiples puentes interdepartamentales que favorecen la eficiencia global de la comunicación. Aquí es más relevante la centralidad de cercanía para facilitar la integración de información en la organización.

En función de estas ideas, el presente trabajo se propone responder a las siguientes preguntas:

- ¿La red de contactos terroristas presenta efectivamente una organización más modular y agrupada que la red de correos corporativos?
- ¿En qué medida difieren los roles de los nodos de alta centralidad entre una red de comunicación formal (Email-EU) y una red clandestina (Terroristas)?
- ¿Qué correlato tiene esta diferencia estructural en la robustez ante ataques dirigidos o fallas?
- ¿Hasta qué punto las comunidades detectadas automáticamente en Email-EU reflejan la estructura funcional real de la organización (departamentos)?

Este abordaje permitirá explorar cómo las exigencias funcionales —seguridad en redes clandestinas vs. eficiencia en redes formales— se manifiestan en la arquitectura global de las redes humanas.

2. Metodología

Para abordar las preguntas que guían este trabajo y obtener una visión integral sobre las similitudes y diferencias estructurales entre redes con propósitos y lógicas comunicacionales tan dispares se optó por un enfoque basado en teoría de grafos.

Se trabajó con dos redes reales: la red Terroristas y la red Email-EU, que se describen en el siguiente punto. Además de analizar estas redes empíricas, se consideraron cuatro modelos clásicos de generación de grafos —Erdős–Rényi (ER), Watts–Strogatz (WS), Barabási–Albert (BA) y Holme-Kim (HK)— como referencias para contrastar sus propiedades.

Para realizar una comparación significativa entre las redes reales y los modelos prototípicos, se ajustaron los parámetros para que coincidan, en la medida de lo posible, con las características estructurales básicas de las redes reales, en particular el número de nodos y enlaces (o densidad).

- **Metodología para la creación de los prototipos** Para el prototipo ER se utilizó la función `nx.erdos_renyi_graph(n, p)` del paquete NetworkX. El valor de p se calculó como $p = \frac{2m}{n(n-1)}$, siendo n el número de nodos de la red real y m la cantidad de enlaces. Esta fórmula deriva del hecho de que el número esperado de enlaces en un grafo ER es $p \cdot \frac{n(n-1)}{2}$, por lo tanto, despejamos p para igualar el número de enlaces esperados al de la red real.

  Para el modelo WS se utilizó la función `nx.watts_strogatz_graph(n, k, p)` donde: k fue estimado como el grado medio de la red real, calculado como $k = \text{round}\left(\frac{2m}{n}\right)$, y ajustado para que sea un número par. p se fijó en 0.03, un valor comúnmente adoptado para

obtener una estructura small-world con alto clustering. Este modelo genera una red regular con k nodos vecinos, con posibilidad de reconexión aleatoria según p (7).

Para el prototipo Barabási–Albert (BA) se utilizó la función `nx.barabasi_albert_graph(n, m)` con m estimado como $m = \text{round}\left(\frac{m_{\text{real}}}{n_{\text{real}}}\right)$. Este valor asegura que la densidad de enlaces en la red generada sea similar a la real. El modelo BA agrega nodos secuencialmente, conectándolos a m nodos existentes según un mecanismo de attachment preferencial(8).

Por último, para el modelo Holme–Kim (HK) se empleó la función `nx.powerlaw_cluster_graph(n, m, p)` con el mismo valor de m utilizado en BA, y p fijado en 0.3. Este modelo extiende BA al incorporar cierre de triángulos locales con probabilidad p, permitiendo generar redes con cola pesada y mayor clustering que BA. El valor de $p = 0{,}3$ se eligió como valor intermedio comúnmente utilizado en la literatura para lograr una triangulación significativa sin destruir la estructura libre de escala(9).

- **Metodología para la generación de instancias de los prototipos en la comparación de clustering y distancias.** Dado que la generación de instancias ER para la red TerroristUnweighted resultó ocasionalmente en grafos no conectados, se procedió a calcular las distancias medias utilizando la componente gigante de esta red cuando fue necesario. En el caso de EmailGiant, no se detectaron errores en el cálculo, por lo que asumimos conectividad suficiente en las instancias generadas.

El análisis se centró en comparar métricas clave de teoría de redes, tales como la distribución de grados, el coeficiente de clustering, los caminos mínimos, la robustez estructural y medidas de centralidad (grado e intermediación). Además, se evaluó la modularidad como criterio para la detección de comunidades dentro de cada red. Para ello, se aplicaron los algoritmos de *Louvain* y *Girvan-Newman*, los cuales permiten identificar particiones óptimas de la red basadas en estructuras comunitarias: el primero mediante la optimización jerárquica de la modularidad y el segundo a través de la eliminación progresiva de enlaces con alta intermediación.

3. Descripción de los datos

3.1. Presentación y contexto

En este trabajo se utilizan dos redes reales de contactos humanos, de naturaleza y contexto muy distintos:

- Email-EU: red de comunicaciones por correo electrónico en una institución europea de investigación. Cada nodo representa una persona y cada enlace representa el intercambio de al menos un correo entre dos individuos. Además, se cuenta con información adicional sobre la pertenencia de cada nodo (persona) a un departamento específico. Dataset Email-EU

- Terroristas: red de contactos entre supuestos terroristas involucrados en los atentados a un tren en Madrid (2004). Cada nodo representa a un individuo, y cada enlace indica la existencia de un contacto entre dos personas, reconstruido a partir de fuentes periodísticas. En este caso, no se dispone de etiquetas adicionales, pero sí con los pesos que indican la cantidad de contactos entre cada nodo. Dataset Terroristas

3.2. Características generales de los datasets

Una primera aproximación a la estructura de estas redes nos entrega la siguiente información (Tabla "Características generales de los grafos analizados"):

Cuadro 1: Características generales de los grafos analizados

	Email-EU	**Terrorist**
Nodos	1005	64
Enlaces	25571	243
Tipo de red	No dirigida	No dirigida
¿Pesada?	No	Sí
¿Conectada?	No	Sí
Densidad	0.0507	0.1206

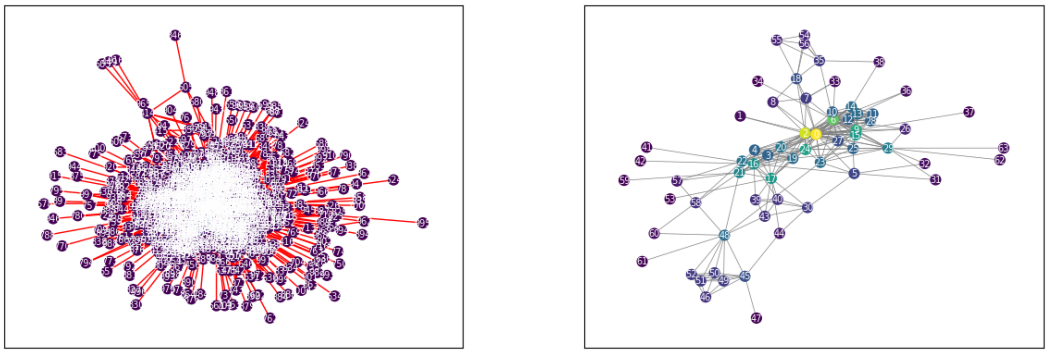
Sin embargo, como la red Email-EU es no conectada, se trabajará con la componente gigante "emailGiant" sin autoenlaces. Además, debido a que la red Terroristas es una red pesada, se quitarán los pesos y se utilizará como red "TerroristUnweighted" sin autoenlaces. Estos nuevos grafos tienen las siguientes características (Tabla: "Propiedades topológicas de los subgrafos analizados"):

Cuadro 2: Propiedades topológicas de los subgrafos analizados

	emailGiant	**TerroristUnweighted**
Nodos	986	64
Enlaces	16064	243
Tipo de red	No dirigida	No dirigida
¿Pesada?	No	No
¿Conectada?	Sí	Sí
Densidad	0.0331	0.1206
Grado promedio $< k >$	32.58	7.59
Nodo con $k_{\text{máx}}$	Nodo 160, grado 345	Nodo 0, grado 29
Nodo con $k_{\text{mín}}$	Nodo 449, grado 1	Nodo 34, grado 1
Coef. de clustering $< C >$	0.41	0.62
Distancia media	2.59	2.69
Eficiencia global	0.42	0.45

La interpretación de estas propiedades motivó las preguntas que guian este trabajo y que fueron planteadas en la Introducción.

Observaciones sobre las propiedades topológicas de ambas redes Una primera diferencia estructural significativa entre los subgrafos analizados es su densidad. Mientras que el subgrafo emailGiant (Figura "Grafos" a) presenta una densidad de 0.0331, TerroristUnweighted alcanza un valor de 0.1206. Esta diferencia sugiere que, en proporción a su tamaño, la red de contactos entre terroristas está mucho más densamente conectada que la red de correos electrónicos (Figura "Grafos" b). Si bien emailGiant cuenta con muchos más nodos y enlaces en términos absolutos, la menor densidad indica una estructura más laxa, con menor probabilidad de conexión entre pares aleatorios de nodos. En cambio, la mayor densidad en TerroristUnweighted puede reflejar una organización más cerrada y altamente interconectada entre miembros, coherente con las necesidades de coordinación en células pequeñas.



(a) emailGiant (b) Terroristas

Figura 1: Grafos

En la red Email-EU se observa una distribución de grados con cola pesada y caída suave cuando se lo visualiza en escala log-log indicando la presencia de múltiples nodos de grado medio-alto (Figura: “Distribución de grado (log)”, versus Figura “Distribución de grado (lineal)”). Esta concentración sugiere una estructura de "mundo pequeño"típica de redes sociales abiertas, donde no solo existen superhubs, sino también varios nodos relevantes en la comunicación. En la red TerroristUnweighted, en cambio, la distribución de grados cae de forma más abrupta. Se detecta un nodo con grado significativamente superior al promedio, lo cual, dado el tamaño reducido del grafo, puede interpretarse como un superhub moderado. Este nodo cumple un rol de conectividad crítica entre células aisladas, en coherencia con la lógica de compartimentación operativa propia de redes clandestinas.

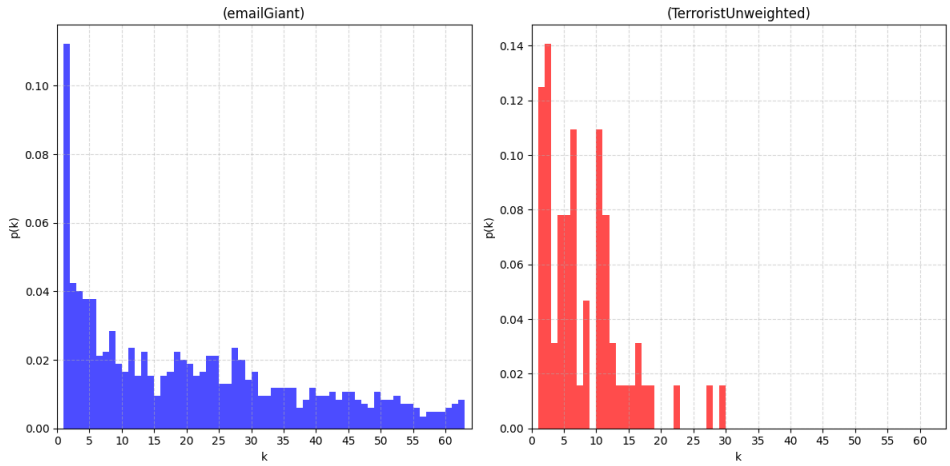


Figura 2: Distribución de grado (lineal)

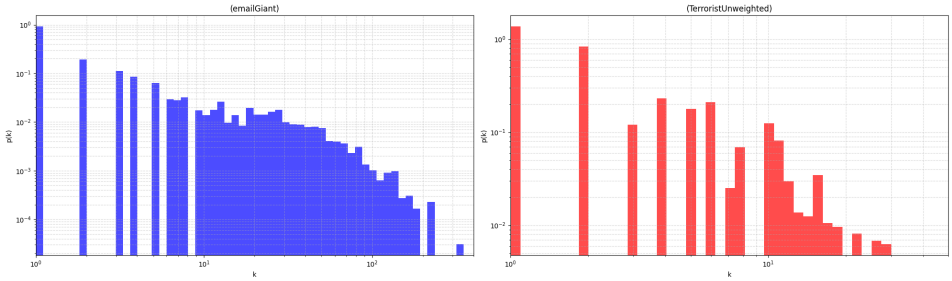


Figura 3: Distribución de grado (log)

Ambas redes presentan coeficientes de clustering relativamente altos, aunque TerroristUnweighted alcanza un valor aún mayor (0.62 frente a 0.41 en emailGiant). Esto sugiere que, en ambos casos, los contactos tienden a formar grupos cerrados, aunque por motivaciones distintas (eficiencia interna en Email-EU, seguridad operativa en Terroristas).

En cuanto a eficiencia global y distancia media, las dos redes muestran distancias mínimas medias cortas, propias de estructuras de tipo "mundo pequeño"que permiten una comunicación o coordinación eficiente. Profundizaremos estas observaciones en las secciones que siguen.

4. Resultados y discusión

4.1. Comparación con prototipos

4.1.1. Distribución de grado

Se comparó la distribución de grado de los datasets con la de una instancia de los prototipos ER, WS, BA y HK ajustando los parámetros con el objetivo de hacer coincidir el número de nodos y enlaces (o densidad) con las redes observadas.

El prototipo ER muestra una distribución de grados altamente concentrada en un valor medio, un comportamiento clásico de este tipo de modelos y que no se parece en nada a la cola de la distribución de emailGiant. El prototipo WS también muestra mucha concentración en un valor medio y no modela bien la dispersión real de grados de emailGiant. El prototipo BA sí tiene una cola pesada como emailGiant, pero con una caída más lineal en la visualización en escala logarítmica, esto es un comportamiento típico del “preferential attachment”. En el caso de emailGiant hay muchísimos nodos de grado medio-alto, en cambio en BA la mayoría de los nodos se quedan con grados bajos y muy pocos se convierten en hubs. Si bien BA es el que más se parece en forma general, tiene menos dispersión y menos clustering que emailGiant (Figura “Distribución de grado (lin) versus (log) comparación prototipos -emailGiant”).

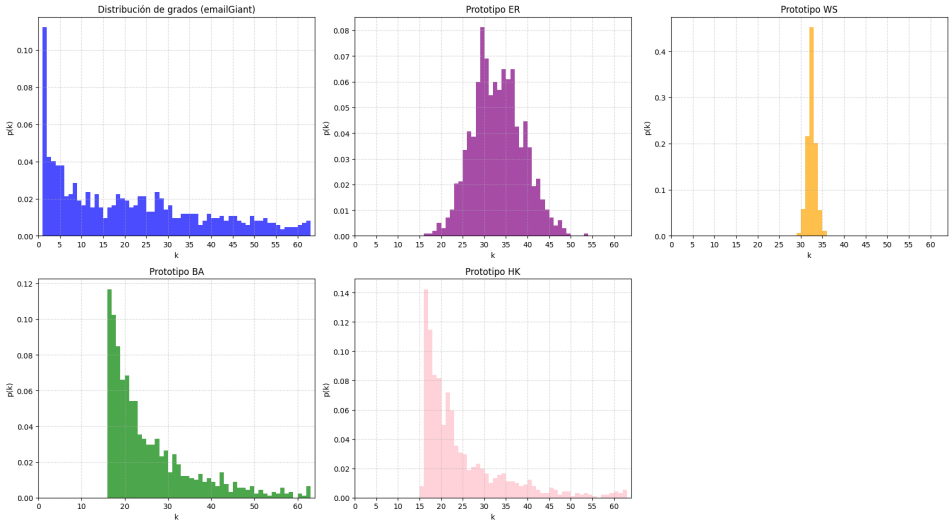


Figura 4: Distribución de grado (lin) - comparación prototipos - emailGiant

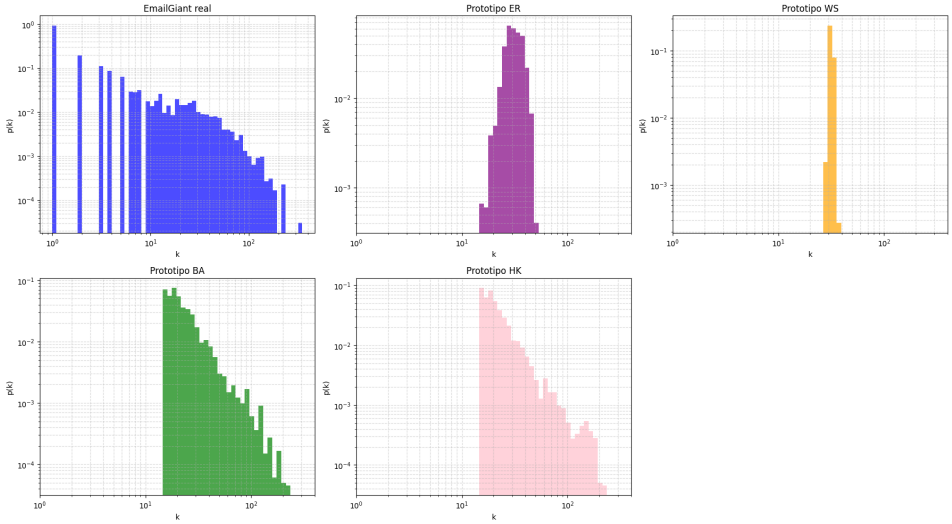


Figura 5: Distribución de grado (log) - comparación prototipos -emailGiant

El prototipo ER está más concentrado en grados bajos con caída abrupta, no refleja bien la distribución de grados más dispersa de TerroristUnweighted. El prototipo WS, que se podría suponer sería más adecuado para redes compartimentadas y homogéneas como la de Terroristas, muestra una distribución extremadamente concentrada que se aleja mucho de la distribución real de la red. El prototipo BA logra modelar más dispersión, sin embargo genera demasiados nodos de grado bajo comparado con la red real. No obstante, es la más parecida de las tres (Figura "Distribución de grado (lin) versus (log) - comparación prototipos - TerroristUnweighted").

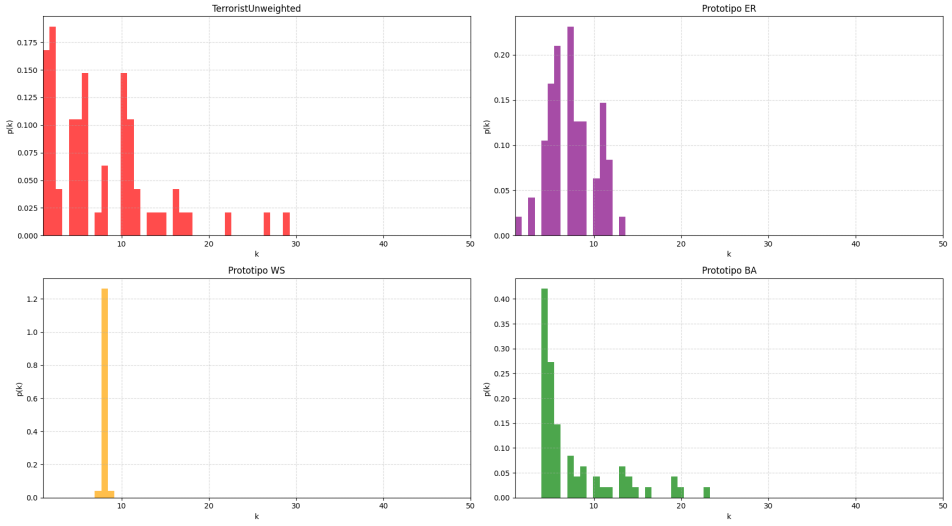


Figura 6: Distribución de grado (lin) - comparación prototipos - TerroristUnweighted

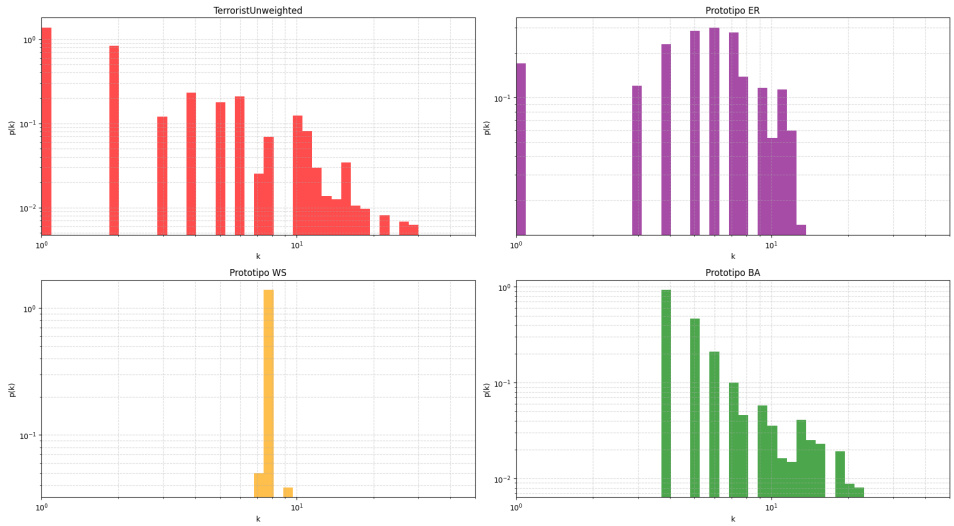
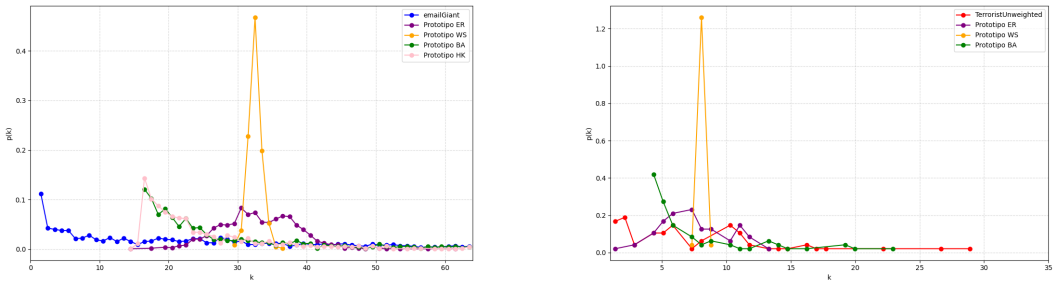


Figura 7: Distribución de grado (log) - comparación prototipos - TerroristUnweighted

Para cerrar esta sección agregamos una visualización diferente de las distribuciones de grado de ambas redes que permite apreciar las observaciones realizadas desde una óptica diferente (Figura “Distribución de grado (lin) -comparación prototipos superpuestos”).



(a) emailGiant

(b) TerroristUnweighted

Figura 8: Distribución de grado (lin) -comparación prototipos superpuestos

4.1.2. Coeficiente de clustering medio y distancia mínima media

Se analizó el coeficiente de clustering medio y la distancia mínima media de los datasets con los de 20 instancias de los prototipos (Cuadros “Clustering medio y distancia mínima” para cada red).

Cuadro 3: Clustering medio y distancia mínima media (comparación con prototipos) emailGiant

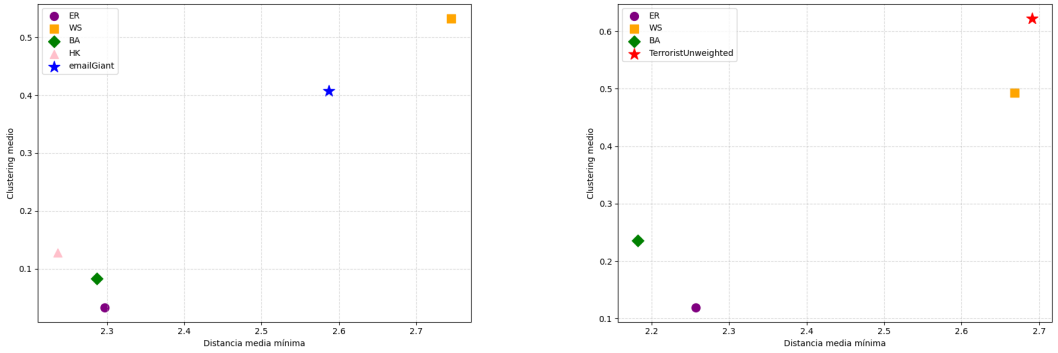
Métrica	**Clustering promedio**	**Distancia mínima media**
emailGiant (real)	0.4071	2.5869
ER (media ± std)	$0{,}0330 \pm 0{,}0007$	$2{,}2982 \pm 0{,}0078$
WS (media ± std)	$0{,}5336 \pm 0{,}0033$	$2{,}7471 \pm 0{,}0047$
BA (media ± std)	$0{,}0831 \pm 0{,}0021$	$2{,}2871 \pm 0{,}0052$
HK (media ± std)	$0{,}1274 \pm 0{,}0025$	$2{,}2377 \pm 0{,}0060$

Cuadro 4: Clustering medio y distancia mínima media (comparación con prototipos) TerroristUnweighted

Métrica	Clustering promedio	Distancia mínima media
TerroristUnweighted (real)	0.6223	2.6910
ER (media ± std)	$0{,}1163 \pm 0{,}0124$	$2{,}2485 \pm 0{,}0498$
WS (media ± std)	$0{,}4784 \pm 0{,}0307$	$2{,}6218 \pm 0{,}0799$
BA (media ± std)	$0{,}2236 \pm 0{,}0265$	$2{,}1921 \pm 0{,}0256$

En el análisis comparativo del coeficiente de clustering medio para ambas redes (emailGiant y TerroristUnweighted), se observan resultados de gran similitud. El modelo WS es el que encuentra un valor más parecido al de las redes reales, los otros prototipos resultan en coeficientes muy bajos de clustering. En cuanto a la distancia mínima media, los valores de todos los modelos son relativamente parecidos, por lo cual no hay una ventaja significativa en la modelización entre los distintos prototipos. Sin embargo, es WS el que más se parece al valor real de ambas redes (Figura "Clustering medio y distancia mínima media comparación con prototipos").

Se incluyó el análisis con el prototipo HK para la red emailGiant y si bien logra expresar un mayor clustering respecto de BA, su valor sigue siendo significativamente inferior al coeficiente de clustering real observado. Además, su distancia mínima media resultó inferior, indicando que tampoco reproduce de manera adecuada la estructura de la red real.



(a) emailGiant (b) TerroristUnweighted

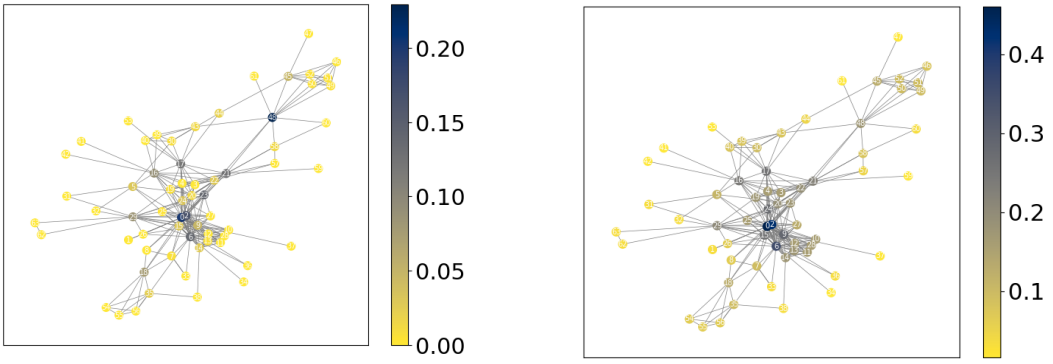
Figura 9: Clustering medio y distancia mínima media (comparación con prototipos)

En resumen, WS produce alto clustering y distancias cortas que se ajustan a las características de las redes observadas. ER, BA y HK no logran reproducir bien esta característica.

La comparación sugiere que ER no modela adecuadamente ninguno de los datasets, dado su bajo clustering y distribución concentrada. WS reproduce razonablemente bien el fenómeno de alto clustering y distancias cortas observado en ambas redes, aunque su distribución de grados no captura la heterogeneidad de ninguna de ellas. BA es el prototipo que mejor expresa la dispersión de las distribuciones de ambas redes aunque con limitaciones. Estas comparaciones muestran que, si bien los prototipos ofrecen intuiciones útiles, las redes humanas reales combinan mecanismos de formación múltiples y modelarlas requiere considerar no solo el grado y la distancia, sino también la modularidad y los roles de los nodos centrales.

4.2. Análisis de centralidad de los nodos

Se determinó la centralidad de intermediaciones y de grado para cada grafo.



(a) Intermediación (b) Grado

Figura 10: Centralidades en Terroristas

A continuacion se listan los nodos con mayor centralidad para cada tipo :

Cuadro 5: Nodos con mayor centralidad -Terroristas

Centralidad de intermediación		**Centralidad de grado**	
Nodo	**Valor**	**Nodo**	**Valor**
48	0.2297	0	0.4603
0	0.2009	2	0.4286
2	0.1643	6	0.3492
23	0.1377	9	0.2857
6	0.1371	24	0.2698
21	0.1262	15	0.2540
17	0.1189	17	0.2540
16	0.0900		

El análisis de centralidades aporta información relevante sobre la estructura interna de las redes:

La centralidad de intermediación revela qué nodos actúan como puentes para el flujo de información entre distintas partes de la red, siendo cruciales para la comunicación intercomunitaria. El nodo 48 tiene el máximo valor de centralidad por intermediación, aunque su valor de centralidad de grado es bajo. Por lo que concluimos que este nodo, de alta centralidad por intermediaciones, no necesariamente tiene muchas conexiones, pero sí conecta grupos separados, funcionando como intermediario de dos posibles comunidades (Figura “Centralidades en Terroristas”).

Por otro lado, la centralidad de grado permite identificar a los individuos con mayor número de conexiones directas, es decir, aquellos con mayor ”popularidad” o contacto dentro de la red. En la red Terrorist, por ejemplo, estos nodos podrían representar actores con una posición clave en la operación logística. Se observa que los nodos con mayor centralidad de este tipo son el nodo 0 y 2, que se encuentran en la zona más densa de la red. Estos nodos también poseen un alto nivel de centralidad por intermediaciones, por lo que representan puntos de gran conexión y por los que circula mucho flujo de información.

No obstante, si bien estas medidas son útiles, ofrecen una visión limitada. Las centralidades no siempre reflejan otros factores importantes como el nivel de jerarquía, el liderazgo efectivo o el poder real dentro de una organización clandestina (10).

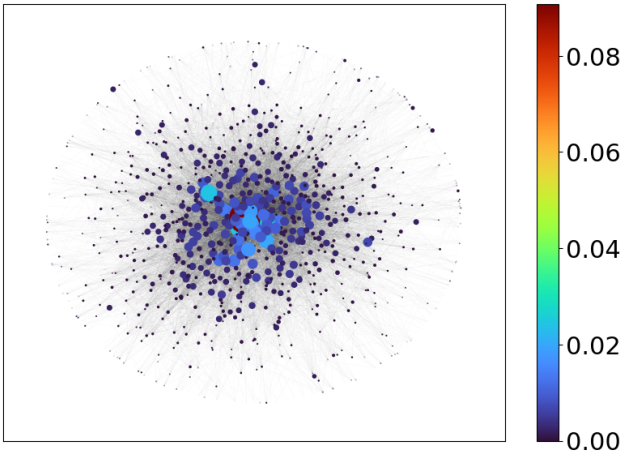


Figura 11: Centralidad de intermediación -emailGiant

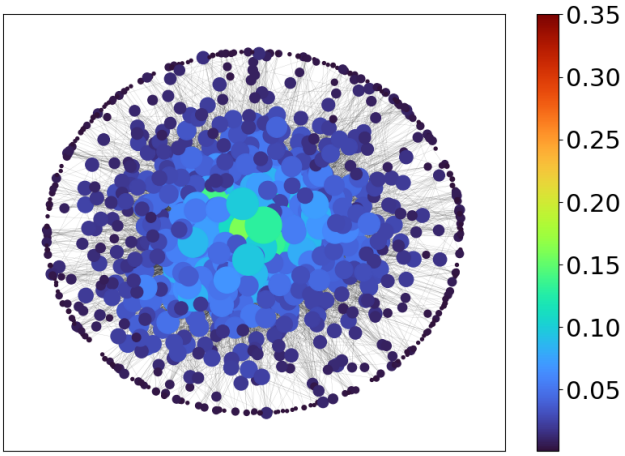


Figura 12: Centralidad de grado -emailGiant

En el grafo de emailGiant, al tener gran cantidad de nodos, la información visual se dificulta, pero podemos observar los nodos con mayor valor de cada centralidad (Figuras “Centralidad de intermediación y de grado -emailGiant” y Cuadro “Nodos con mayor centralidad -emailGiant”).

Cuadro 6: Nodos con mayor centralidad -emailGiant

Centralidad de intermediación		**Centralidad de grado**	
Nodo	**Valor**	**Nodo**	**Valor**
160	0.0908	160	0.3503
86	0.0393	121	0.2355
5	0.0322	82	0.2345
82	0.0290	107	0.2223
121	0.0289	86	0.2193
		62	0.2173
		434	0.1858

En este grafo, caracterizado por el número elevado de nodos, la mayoría de ellos tienen valores bajos de intermediación, lo cual es normal, ya que hay muchísimos caminos posibles entre pares de nodos,

y muy pocos nodos concentran el tráfico. En cambio, la centralidad de grado escala más rápido en grafos grandes. Hay más nodos con valores relativamente medio-altos de centralidad de grado, por lo que podríamos pensar la existencia de hubs o nodos muy conectados, lo que coincide con el análisis del punto anterior en donde se observó la presencia de muchos nodos de grados medios y altos.

4.3. Análisis de robustez de los grafos

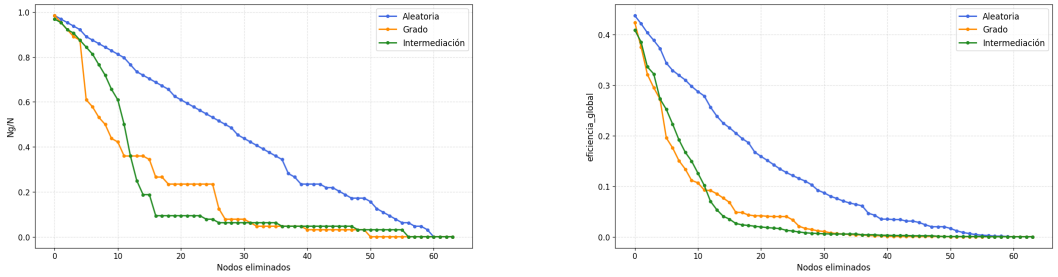
Para cuantificar la robustez estructural de las redes ante diferentes escenarios de perturbación, se implementó un procedimiento basado en la eliminación progresiva de enlaces asociados a nodos, desconectando al nodo de la red. Esta aproximación permite evaluar la degradación funcional sin modificar el conjunto de nodos activos.

En cada iteración, se calculan dos indicadores clave:

- **Tamaño relativo de la componente gigante** (N_g/N): proporción de nodos que permanecen conectados dentro del mayor componente conexo respecto del número total original.
- **Eficiencia global**: medida de la eficiencia promedio de la comunicación entre todos los pares de nodos, considerando las longitudes de los caminos más cortos en la red restante.

Este análisis se repite para tres estrategias distintas de eliminación de enlaces: aleatoria (fallos no dirigidos), según centralidad de grado del nodo y según centralidad de intermediación del nodo (ataques dirigidos). La comparación entre estas estrategias permite caracterizar la vulnerabilidad diferencial de las redes ante perturbaciones espontáneas versus ataques estructurados.

4.3.1. Robustez en red Terroristas



(a) Tamaño relativo de la comp. gig. (N_g/N)

(b) Eficiencia global

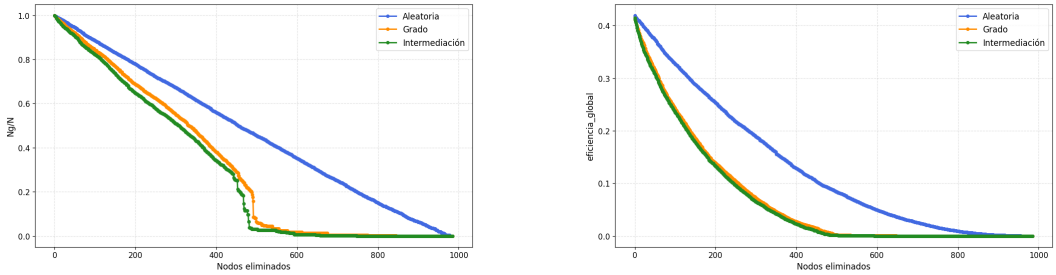
Figura 13: Comparación de la robustez estructural de la red *TerroristUnweighted* frente a tres estrategias de eliminación de enlaces.

Como se observa en la Figura "Comparación de la robustez estructural de la red *TerroristUnweighted* frente a tres estrategias de eliminación de enlaces", al eliminar nodos al azar (línea azul), el tamaño relativo de la componente gigante (N_g/N) disminuye de forma progresiva, evidenciando cierta resiliencia frente a fallos aleatorios. La eficiencia global cae también de forma suave, lo que sugiere que la red puede tolerar pérdidas no dirigidas sin un colapso inmediato.

En contraste, los ataques dirigidos —tanto por grado (línea naranja) como por intermediación (línea verde)— provocan una caída abrupta de N_g/N y de la eficiencia global. Esto revela que la red está fuertemente sostenida por unos pocos nodos clave, cuya eliminación fragmenta rápidamente la estructura. El comportamiento similar entre grado e intermediación sugiere que los nodos más conectados también ocupan posiciones centrales en la red, función común en redes pequeñas o densas.

La red de terroristas presenta una alta robustez ante fallos aleatorios, pero una alta fragilidad estructural frente a ataques dirigidos, lo que concuerda con redes altamente organizadas y dependientes de hubs o nodos puente. Estos resultados coinciden con hallazgos previos en análisis de redes terroristas, donde la centralidad de ciertos actores los vuelve puntos críticos para la cohesión estructural de la red (10).

4.3.2. Robustez en red Email-EU



(a) Tamaño relativo de la comp. gig. (N_g/N)

(b) Eficiencia global

Figura 14: Comparación de la robustez estructural de la red *emailGiant* frente a tres estrategias de eliminación de enlaces.

La red emailGiant muestra una disminución progresiva y casi lineal del tamaño de la componente gigante bajo eliminación aleatoria (Figura “Comparación de la robustez estructural de la red *email-Giant* frente a tres estrategias de eliminación de enlaces”). Esto sugiere una estructura robusta frente a fallos no dirigidos, característica de redes complejas con redundancia estructural.

Sin embargo, al aplicar estrategias dirigidas (grado o intermediación), se observa una caída mucho más acelerada tanto en N_g/N como en la eficiencia global. En particular, la eliminación basada en grado provoca un descenso más abrupto en las etapas iniciales, mientras que la intermediación tiene un impacto ligeramente más gradual.

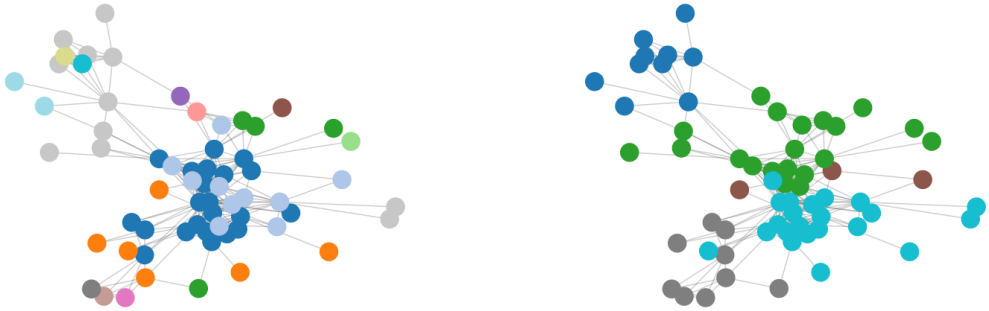
Este comportamiento es coherente con redes con hubs múltiples y estructuras descentralizadas, como las redes libres de escala descritas por Barabási-Albert (8), donde la conectividad general persiste ante fallos aleatorios pero colapsa ante ataques a nodos clave. A diferencia de la red Terroristas, la red Email-EU tolera mejor los ataques dirigidos durante más tiempo, aunque termina cediendo ante ataques suficientemente prolongados.

En conjunto, los resultados reflejan que la red Email-EU posee una robustez superior a la red Terroristas, aunque sigue siendo vulnerable ante ataques estratégicos sobre nodos de alta centralidad.

4.4. Comunidades en los grafos

4.4.1. Partición óptima según modularidad para grafo de terroristas

El algoritmo de Girvan-Newman identificó 15 comunidades con una modularidad menor (0.396), lo que indica una división más granular pero menos eficaz en términos de cohesión interna (11). En la Figura ”Comparación de las comunidades obtenidas Terroristas -con algoritmo de Girvan Newman", se puede observar que la red aparece más fragmentada, con comunidades pequeñas y conexiones entre ellas más difusas. Esta partición puede capturar subestructuras locales, pero presenta menor claridad en la separación global de la red (12).



(a) Con algoritmo de Girvan-Newman con modularidad de 0.396

(b) Con algoritmo de Louvain con modularidad de 0.448

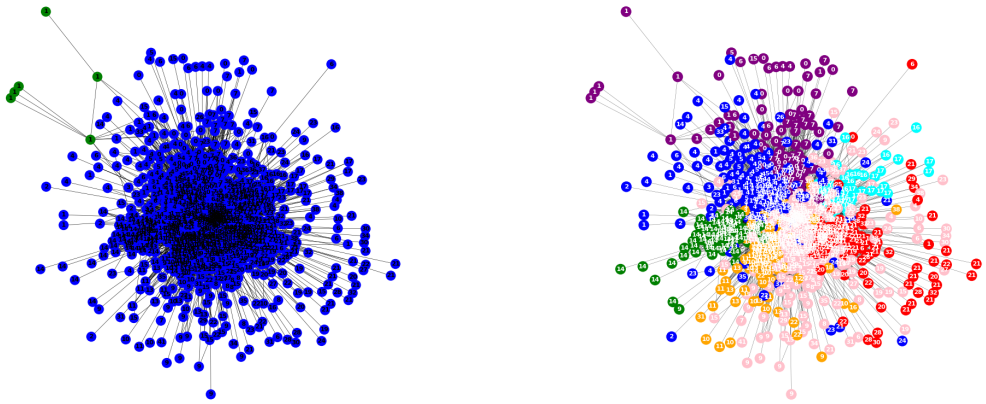
Figura 15: Comparación de las comunidades obtenidas -Terroristas

Por otro lado, el algoritmo de Louvain detectó 5 comunidades en la red Terroristas, con una modularidad de 0.448. Esta partición sugiere una estructura bien modular, donde los nodos están densamente conectados dentro de sus comunidades y presentan pocos enlaces entre grupos. La visualización en la Figura ”Comparación de las comunidades obtenidas Terroristas -con algoritmo de Louvain” refleja bloques claramente diferenciados, lo que indica cohesión interna en cada comunidad y una segmentación funcional de la red (13).

4.4.2. Partición óptima según modularidad para grafo de email-EU

El algoritmo de Girvan–Newman identificó 2 comunidades en la red de correos electrónicos, con una modularidad extremadamente baja (0.0006), Figura ”Comparación de las Comunidades obtenidas -emailGiant, con algoritmo de Girvan-Newman con modularidad de 0.0006”. Esto se debe a que el grafo de emails tiene una densidad baja (3.31 % de las conexiones posibles entre nodos), para este caso, el algoritmo no ha logrado dividir la red de forma efectiva, lo que impide realizar un análisis (11).

En contraste, el algoritmo de Louvain detectó 7 comunidades con una modularidad superior (0.410). Este valor refleja una partición más coherente desde el punto de vista estructural, donde los nodos tienden a concentrar sus conexiones dentro de sus respectivas comunidades. La visualización en la Figura Çomparación de las Comunidades obtenidas -emailGiant, con algoritmo de Louvain con modularidad de 0.410"muestra conglomerados bien diferenciados, lo que indica una segmentación más funcional de la red. La visualización muestra una estructura bien dividida en grupos, donde los nodos de cada comunidad están fuertemente conectados entre sí y tienen pocas conexiones con otros grupos (13).



(a) Con algoritmo de Girvan-Newman con modularidad de 0.0006

(b) Con algoritmo de Louvain con modularidad de 0.410

Figura 16: Comparación de las comunidades obtenidas -emailGiant

Para concluir este capítulo, ambas redes, la de terroristas y la de correos electrónicos, presentan modularidades cercanas a 0.4. Esto sugiere que, en ambos casos, los nodos tienden a agruparse en comunidades bien definidas (13), con muchas conexiones internas y pocas hacia otros grupos. En términos estructurales, ambas redes comparten un patrón de organización similar.

5. Conclusiones

Este trabajo permitió estudiar dos redes sociales de naturaleza muy diferente: una red clandestina (Terrorist) y una red institucional (Email-EU).

A través de análisis y comparaciones con modelos prototipo, se observó que ambas redes presentan un alto coeficiente de clustering y distancias cortas, características propias de redes del tipo "small world". Sin embargo, difieren significativamente en su distribución de grados y en su respuesta a fallos o ataques.

La red de terroristas muestra una fuerte centralización en pocos nodos críticos, lo que la hace altamente vulnerable a ataques dirigidos, pero resistente a fallos aleatorios. Esta propiedad es coherente con la necesidad operativa de mantener la funcionalidad del grupo aun si se pierde parte de la red.

Por otro lado, la red de correos electrónicos presenta una estructura más distribuida, con muchos nodos de grado medio-alto, lo que le confiere una robustez mayor y una dependencia menos extrema de hubs individuales.

Estas diferencias reflejan las necesidades funcionales de cada tipo de red: en la clandestinidad, la eficiencia y la compartimentación priman; en entornos institucionales, la redundancia y la conectividad son más valoradas.

Sin embargo, ambas redes comparten similitudes al evaluar su modularidad. En ambas se destaca la presencia de comunidades bien definidas, resaltando, así, la importancia de la estructura comunitaria como un rasgo fundamental en la organización de redes sociales, independientemente de su naturaleza clandestina o institucional.

El análisis de este trabajo demuestra cómo la estructura topológica de una red está profundamente ligada a su contexto social y funcional, y cómo herramientas de la teoría de redes complejas permiten revelar estas lógicas subyacentes.

Referencias

[1] Zech, S. T., & Gabbay, M. (2016). Social Network Analysis in the Study of Terrorism and Insurgency. *International Studies Review*, 18(2).

[2] Clark, C. R. (2016). *Modeling and Analysis of Clandestine Networks*. Air Force Institute of Technology. https://scholar.afit.edu/etd/3772/

[3] Campbell, J. A. (2016). Social Network Analysis with Content and Graphs. MIT Lincoln Laboratory. https://www.ll.mit.edu/sites/default/files/publication/doc/social-network-analysis-content-graphs-campbell-ja-22727.pdf

[4] Diesner, J., & Carley, K. M. (2005). Using Network Text Analysis to Detect the Organizational Structure of Covert Networks. *IEEE Intelligent Systems*, 20(5).

[5] Kumar, S., & Gupta, M. (2022). Analyzing the Email Communication Network of a European Research Institution. *International Journal of Scientific Research in Mathematical and Statistical Sciences*, 9(2), 56–61.

[6] Clarke, R., & Preece, J. (2019). A Network Analysis of Organizational Email Communication: Applications and Ethical Challenges. *Social Sciences*, 8(11), 306. doi:10.3390/socsci8110306

[7] Watts, D. J., & Strogatz, S. H. (1998). Collective dynamics of 'small-world' networks. Nature, 393(6684).

[8] Barabási, A.-L., & Albert, R. (1999). Emergence of Scaling in Random Networks. Science, 286(5439).

[9] Holme, P., & Kim, B. J. (2002). Growing scale-free networks with tunable clustering. Physical Review E, 65(2), 026107.

[10] Perliger, A., & Pedahzur, A. (2006). Social network analysis and counter-terrorism: measuring the impact of centrality.

[11] Girvan, M., & Newman, M. E. J. (2002). Community structure in social and biological networks. *Proceedings of the National Academy of Sciences*, 99(12), 7821–7826.

[12] Newman, M. E. J. (2004). Fast algorithm for detecting community structure in networks. *Physical Review E*, 69(6), 066133.

[13] Blondel, V. D., Guillaume, J. L., Lambiotte, R., & Lefebvre, E. (2008). Fast unfolding of communities in large networks. *Journal of Statistical Mechanics: Theory and Experiment*, 2008(10), P10008.