Más allá de los hubs: ¿Curiosidad computacional para detectar vulnerabilidades ocultas?

Patricio Gerpe Pablo Silvarredonda Ricardo Amarilla
Data Mining en Ciencia y Tecnología

Facultad de Ciencias Exactas y Naturales
Universidad de Buenos Aires
16 de Junio de 2025

Abstract

El estudio de la resiliencia en redes complejas tradicionalmente se ha centrado en analizar fallos en nodos altamente conectados, dejando de lado vulnerabilidades potenciales en nodos estructuralmente menos relevantes. Este trabajo explora la hipótesis de que ciertos nodos periféricos podrían desempeñar roles críticos no evidentes en la robustez del sistema. Combinando herramientas de teoría de redes con enfoques de curiosidad computacional —que emulan procesos del pensamiento lateral humano—, se propone una metodología alternativa para identificar puntos frágiles atípicos. Se analizan dos redes reales con topologías contrastantes: una red social (Facebook) y una red de infraestructura (aeropuertos de EE. UU.), sometiéndolas a dos simulaciones de ataques, una dirigida y otra basada en caminatas aleatorias sesgadas hacia nodos de baja centralidad. Los resultados revelan que si bien las características topológicas exploradas sugerían que la red de aeropuertos podría ser susceptible a ataques no convencionales, una estrategia de curiosidad de caminata aleatoria sesgada hacía nodos de baja centralidad de grado no parecería poder descubrir riesgos no triviales ni relevar anomalías. De hecho, nuestro experimento sugiere que las estrategias convencionales poseen mayor eficacia tanto en una red de mayor heterogeneidad y menor dependencia de hubs como aeropuertos como en una red hub-dependiente como Facebook.

1. Introducción

El exponencial aumento de la complejidad de la interconexión entre sistemas en dominios como las redes sociales y de transporte ha facilitado la disponibilidad y análisis de grandes volúmenes de datos. Estas redes constituyen un insumo clave para la minería de datos en ciencia y tecnología, dado su potencial para modelar fenómenos sociales, tecnológicos y económicos interdependientes. En este contexto, el estudio de la resiliencia de sistemas interconectados cobra creciente relevancia: comprender cómo estas redes resisten perturbaciones es fundamental para anticipar colapsos sistémicos, ya sea en redes sociales, infraestructuras críticas o sistemas ecológicos. Tradicionalmente, los estudios de robustez se han centrado en ataques a nodos altamente conectados, asumiendo que son los puntos más vulnerables. Sin embargo, esta aproximación puede pasar por alto configuraciones críticas no evidentes, donde nodos aparentemente marginales podrían desencadenar disrupciones sistémicas. Por tal razón, nos motiva identificar estas vulnerabilidades ocultas para diseñar infraestructuras más resilientes, especialmente en contextos donde los ataques convencionales podrían omitir riesgos no evidentes que terminen siendo críticos.

En los estudios clásicos de robustez de redes, se recurre habitualmente a simulaciones de ataques aleatorios o dirigidos a nodos de alta centralidad (hubs), lo cual revela las vulnerabilidades más obvias, pero descuida configuraciones atípicas que podrían desencadenar fallos inesperados, Freitas., et al [1]. Para superar estas limitaciones, han emergido enfoques de búsqueda creativa en redes sociales, como Socialz [2], que utilizan algoritmos evolutivos guiados por novedad para simular comportamientos de usuarios no convencionales y descubrir errores que escapan a las pruebas tradicionales, Zanartu., et al

[3]. De manera similar, en redes de transporte, herramientas de monitoreo dinámico de la centralidad de intermediación permiten anticipar cuellos de botella antes de que se materialicen en situaciones reales de congestión, Furno et al., [4]. Más aún, las heurísticas de curiosidad computacional, implementadas por ejemplo en AutoOD, exploran de forma no determinísticos patrones inusuales en datos complejos, Li et al., [5], y marcos adversariales como VCAT incorporan recompensas por novedad para revelar vectores de ataque inéditos en vehículos autónomos, Cai et al., [6].

Por ende, acá nos proponemos evaluar empíricamente la eficacia comparativa de dos estrategias de ataque en redes con topologías contrastantes: (1) un método clásico que ataca primero los nodos centrales y (2) una heurística de curiosidad computacional que sesga la búsqueda hacia nodos periféricos y topológicamente atípicos. Para cada red, una subred de Facebook y la componente gigante binarizada de una red global de conexiones aéreas, llevaremos a cabo dos simulaciones con estrategias diferenciales (convencional vs. curiosa), midiendo para cada simulación, variaciones tanto la conectividad global (tamaño relativo de la componente gigante) como en la eficiencia global. El objetivo de estas simulaciones será identificar patrones diferenciales de fragilidad ante los dos tipos de ataques.

Para facilitar la claridad de la exposición, el artículo se organiza en las siguientes secciones: (A) Métodos – Describe en detalle las dos estrategias de ataque comparadas, el análisis exploratorio preliminar a realizar sobre las redes analizadas (Facebook y aeropuertos) y las métricas de evaluación empleadas. (B) Resultados y Discusión – Presenta los hallazgos principales, contrastando la efectividad de ambos métodos para identificar vulnerabilidades, y analiza las implicaciones de estos resultados en el contexto de redes con diferentes topologías. (C) Conclusiones – Sintetiza las contribuciones clave del estudio, reflexiona sobre sus limitaciones y propone futuras líneas de investigación para extender este trabajo. El objetivo del presente informe es esclarecer si una estrategia de ataque aleatoria con sesgo hacia nodos de baja de centralidad puede o no puede detectar vulnerabilidades anomalas que no podrían ser detectadas por un ataque convencional como una estrategia dirigida clásica.

2. Métodos

2.1. Diseño Experimental

Con el objetivo de discernir si vulnerabilidades no evidentes pueden ser reveladas mediante una búsqueda atípica, el estudio compara dos estrategias de ataque:

1. **Enfoque clásico**: Eliminación progresiva borrando primero los enlaces de los nodos con mayor centralidad de grado.
2. **Heurística de curiosidad**: Recorrido aleatorio con sesgo hacia nodos de bajo grado. El sesgo aplicado utiliza una razón de probabilidad 1.0/0.1.

$$Razndeprobabilidad = \frac{p_{min}}{p_{max}} = \frac{1{,}0}{0{,}1} = 10$$

La misma se implementó en el siguiente código:

```
def estrategia_curiosa(G, centralidad_dict):
    valores = list(centralidad_dict.items())
    valores.sort(key=lambda x: x[1])  # orden ascendente
    nodos = [x[0] for x in valores]
    pesos = np.linspace(1.0, 0.1, len(nodos))  # sesgo hacia baja centralidad
    pesos /= pesos.sum()
    return random.choices(nodos, weights=pesos, k=len(nodos))
```

Bajo este sesgo, el nodo con menor centralidad tiene 10 veces más chances de ser elegido que el de mayor centralidad. De todas las posibles medidas de centralidad, optamos por la centralidad de grado. Creemos que esta métrica provee información crítica para nuestro informe puesto que nos revela aquellas zonas típicamente priorizadas por estrategias tradicionales donde se concentran más nodos. Futuras investigaciones podrían contemplantar un índice con distintas medidas de centralidad tal como grado e intermediación, y explorar dichas estrategias en un más variado conjunto de topologías (como experimentar con redes pesadas y direccionadas).

2.2. Datasets y Preprocesamiento

Para aplicar tales estrategias, se seleccionaron redes representativas de dominios contrastantes (comunicación y transporte) dado que presentan topologías diferentes en las cuáles podríamos esperar dinámicas de fallo críticamente distintas.

Facebook: Este grafo representa círculos de amistad en la plataforma Facebook. Los datos fueron recolectados mediante una encuesta anónima que capturó relaciones de amistad entre usuarios. Cada nodo representa un perfil individual de usuario, y cada arista no dirigida indica la existencia de una relación de amistad mutua entre dos usuarios. El grafo cuenta con 4039 nodos y 88.234 enlaces, lo que refleja un nivel considerable de interconexión social. Se trata de una red no dirigida, no ponderada y conexa, lo que implica que existe un camino entre cualquier par de nodos en el grafo.

Aeropuerto: Este grafo dirigido y ponderado representa rutas aéreas entre aeropuertos de Estados Unidos durante el año 2010. Cada nodo corresponde a un aeropuerto, y cada arista dirigida representa la existencia de vuelos programados desde un aeropuerto origen hacia un destino específico. El peso asignado a cada arista indica la cantidad total de vuelos realizados en esa ruta durante el año. La red contiene 1574 nodos y 28.236 enlaces dirigidos, y se caracteriza por ser disconexa, tanto en términos de conectividad fuerte como de conectividad débil. Esto implica que no existe un camino (ni siquiera ignorando la dirección de los enlaces) que conecte a todos los nodos entre sí.

Cuadro 1: Características de las redes analizadas

Propiedad	Facebook	Aeropuertos
Nodos	4,039	1,402 (componente gigante)
Aristas	88,234	17,013 (binarizada)
Tipo	Social	Infraestructura
Distribución de grado	Libre de escala	Ley de potencia truncada

Transformaciones aplicadas:

- *Aeropuertos*: De manera tal que podamos realizar una comparación homogénea entre ambas redes, se optó por realizar una binarización y uso de la componente gigante de la red de Aeropuertos. Entendemos que de esta manera se sacrifica especificidad de dirección/peso, pero al mismo tiempo así permitimos un análisis estructural puro. Cabe aclarar que se eliminaron los pesos sin aplicar umbrales, conservando todas las conexiones y, por ende, la densidad original del grafo.

2.3. Análisis Exploratorio Previo

Antes de implementar las estrategias de ataque, se llevó a cabo un análisis exploratorio estructural con el fin de comprender mejor las propiedades topológicas de las redes originales, evaluar la adecuación de prototipos teóricos como modelos de referencia y así preveer que podríamos esperar encontrar al aplicar cada simulación.

1. **Comparación topologica** Para evaluar la robustez estructural y detectar vulnerabilidades potenciales en las redes analizadas, se implementó una comparación sistemática entre algunas propiedades topológicas de la red de Aeropuertos y la red social de Facebook. La metodología combinó análisis visuales y métricas cuantitativas. Se calcularon y compararon métricas topológicas que encontramos relevantes tal como coeficientes de clustering y grados promedio puesto que nos ofrecen información sobre potenciales concentraciones de fallos en las redes. Al analizar estos indicadores, buscamos identificar patrones diferenciales de organización y resiliencia que nos permitan preveer que esperar al aplicar cada estrategía de ataque.
2. **Comparación de simulaciones de prototipos.**
   De manera tal que podamos evaluar como podrían adecuarse nuestros descubrimientos de cada red a evaluar con prototipos generalizados de redes, realizamos simulaciones de modelos.
   - **Metodología implementada para realizar las simulaciones.**
     Parámetros de entrada. Antes de las simulaciones, se calcularon dos parámetros clave a partir de cada red real:
     - **Número de nodos**: se obtuvo directamente del grafo real.
     - **Grado medio**: se utilizó como referencia para garantizar que las redes sintéticas tuvieran una densidad de enlaces comparable.

Además, se calculó un parámetro denominado *mcero*, necesario para el modelo Barabási-Albert. Este parámetro define el número de enlaces que se añaden en cada paso del modelo de crecimiento preferencial, permitiendo mantener la estructura de red realista.

Modelos utilizados y simulaciones. Para cada grafo bajo estudio, se realizaron simulaciones con los tres modelos de redes aleatorias:

Modelo Barabási-Albert (BA). Este modelo genera redes de crecimiento con conexión preferencial. Para asemejarse a la red real:

- Se utilizó el mismo número de nodos que el grafo real.
- Se calculó el parámetro *mcero* a partir del grado medio real, de modo que cada nuevo nodo agregado tuviera aproximadamente la misma cantidad de enlaces que un nodo promedio.

Esto permitió que las redes generadas tuvieran un grado medio y una densidad de enlaces similares a las reales, asegurando comparaciones significativas.

Modelo Erdős-Rényi (ER). Este modelo crea redes aleatorias donde cada par de nodos se conecta con igual probabilidad. Para replicar la densidad de enlaces:

- Se fijó el mismo número de nodos que el grafo real.
- Se ajustó el número de aristas al valor observado en la red real.

De esta manera, las redes ER simuladas conservaron la misma densidad promedio de conexiones que la red real, facilitando la comparación de métricas como el clustering y la distancia promedio.

Modelo Watts-Strogatz (WS). Este modelo genera redes de "pequeño mundo", intermedias entre redes regulares y aleatorias. Para asemejarse a la red real:

- Se utilizó el mismo número de nodos.
- Se determinó el número de vecinos iniciales de cada nodo a partir del grado medio real, garantizando una conectividad local similar.
- Se usó una probabilidad de reconexión baja (0.03) para introducir aleatoriedad y mantener la estructura local.

Esto permitió que las redes simuladas conservaran características similares a la red real tanto en conectividad local como en estructura global.

Con estos ajustes, cada modelo generó redes sintéticas que imitaban las propiedades estructurales básicas del grafo real de aeropuertos. Así, se aseguraron comparaciones válidas y relevantes para evaluar la idoneidad de los modelos teóricos en la representación de redes reales.

Ejecución de las simulaciones de prototipos. Para cada modelo, se realizaron 1000 simulaciones independientes para garantizar la robustez estadística de los resultados. Estas simulaciones se implementaron en paralelo mediante la librería `joblib`, optimizando el uso de múltiples núcleos de procesamiento. Los resultados se guardaron en archivos utilizando `pickle`, y se implementó un mecanismo de guardado incremental por bloques para evitar la pérdida de datos en caso de interrupciones.

3. **Análisis de centralidad.**

   Se calcularon métricas de centralidad de grado para todos los nodos en ambas redes, como paso necesario para implementar ambas estrategias de ataque. Este análisis también sirvió como diagnóstico de la jerarquía estructural implícita en la red, y permitió anticipar posibles puntos de falla clave. Como complemento de análisis topológico, cálculamos algunas métricas de centralidad adicionales que, si bien no se implementan en las simulaciones de ataque, su comparación nos brindan información adicional sobre las potencialidades de falla de cada red mientras obtenemos de esto una caracterización más detallada de dichas redes.

4. **Detección de comunidades.**

   Con el objetivo de evaluar la cohesión estructural de las redes y preveer posibles puntos de fragmentación, se aplicaron algoritmos de detección de comunidades. Por un lado, se utilizó el algoritmo de Louvain para identificar particiones óptimas según modularidad. Se reportaron los valores de modularidad obtenidos y se visualizaron las comunidades detectadas. Por otro lado, se replicó el análisis con el algoritmo de Girvan-Newman para comparar la estabilidad y consistencia de la partición obtenida. Realizamos este análisis en búsqueda de evidencia sobre la robustez de estructuras mesoscópicas (comunidades) ante perturbaciones locales.

Dado que el algoritmo de Girvan–Newman tiene un alto costo computacional y no escala bien para grafos grandes, se adoptaron varias medidas prácticas para hacerlo ejecutable en un entorno real. El experimento se realizó en un servidor Amazon EC2, configurado con un entorno virtual que garantizó la disponibilidad de dependencias y el aislamiento de ejecución. Las redes bajo estudio fueron cargadas desde archivos de texto y procesadas con la librería `networkx`. El script fue ejecutado en segundo plano utilizando `nohup`, permitiendo continuar el análisis incluso si se cerraba la sesión. En cada iteración del algoritmo se calcularon dos métricas clave: el número de comunidades generadas y el valor de modularidad correspondiente. Estos datos se registraron en un archivo CSV, lo que permitió realizar un seguimiento completo de la evolución del proceso. Además, la mejor partición encontrada fue almacenada automáticamente en formato `.pkl`, conservando aquella con la modularidad máxima alcanzada hasta el momento. Estas decisiones permitieron ejecutar el análisis de comunidades con Girvan–Newman de forma controlada y reproducible, priorizando resultados útiles sin agotar los recursos disponibles.

El proceso de maximización de la modularidad mediante el algoritmo de **Girvan–Newman** tuvo una duración total de **10 horas** para la red de **Aeropuertos** y de **32 horas** para la red de **Facebook**. La **modularidad máxima** se alcanzó en la **iteración 168** para Aeropuertos y en la **iteración 8** para Facebook. Ver imagen más abajo.

2.4. Métricas de Evaluación

Las métricas se eligieron para capturar tanto la resiliencia global como patrones locales de fragilidad (Tabla 2).

Cuadro 2: Métricas de robustez y su relevancia

Métrica	**Justificación**
Tamaño relativo de la componente gigante (Ng/N)	Efecto en la conectividad global
Eficiencia global	Capacidad de comunicación en redes parcialmente conectadas

A continuación detallaremos los resultados de este artículo, comenzando por el análisis exploratorio preliminar de cada red y finalizando con los hallazgos encontrados luego de implementar las estrategias de ataque evaluadas.

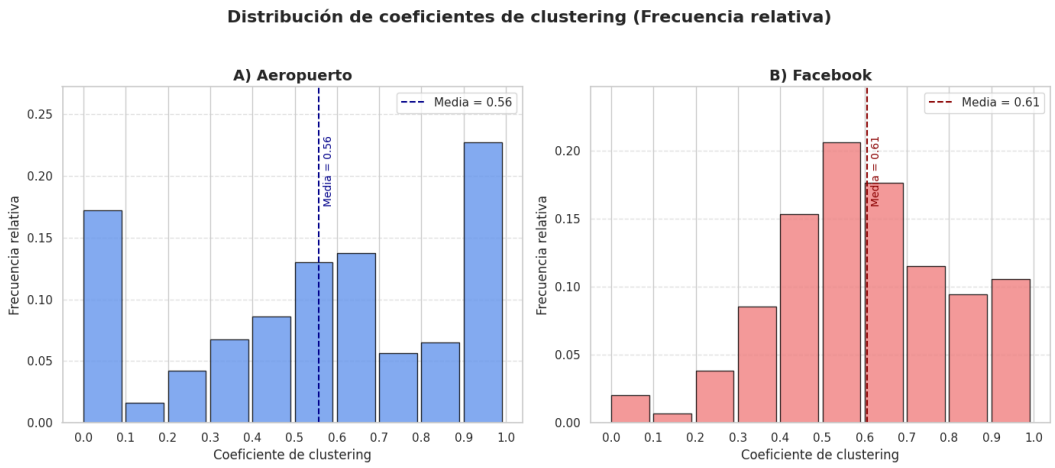
3. Resultados y discusión

3.1. Análisis Exploratorio preliminar

3.1.1. Comparación de la red de Aeropuertos y red social Facebook

Para identificar vulnerabilidades no evidentes y evaluar rigurosamente la robustez de nuestras dos redes bajo análisis, como primer paso resultó fundamental la caracterización precisa de las propiedades topológicas mediante análisis comparativos con modelos teóricos.

3.1.2. Medidas topológicas comparativas



(a) Distribución de coeficientes de clustering

Figura 1: Distribución de Coeficientes de Clustering.

Cuadro comparativa de métricas

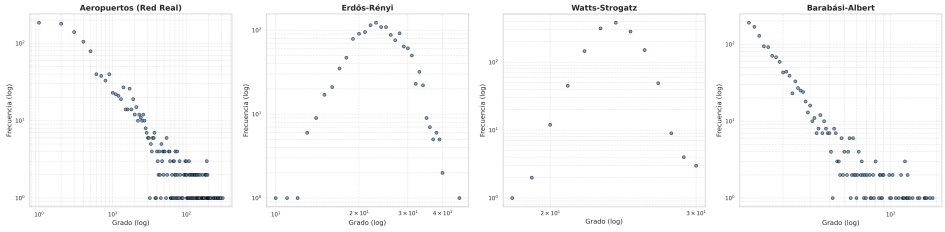
Métrica	Aeropuertos (Componente Gigante Binarizada)	Facebook
Nº de nodos	1402	4039
Nº de enlaces	17013	88234
Grado promedio	24.2696	43.6910
Distancia promedio $\langle d \rangle$	3.0217	3.6925
Distancia máxima (diámetro)	8.0000	8.0000
Clustering promedio (C)	0.5575	0.6055

Figura 2: Comparación de métricas de las redes de Aeropuertos(Componente Gigante Binarizada) y Facebook.

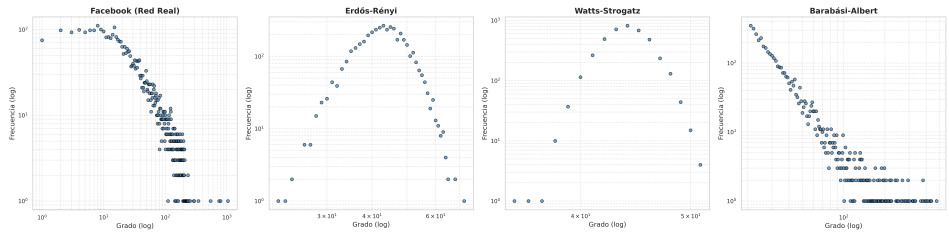
Nos motivó averiguar el coeficiente de clustering y su distribución puesto a que la conectividad que tienen los vecinos de los nodos nos puede dar información adicional sobre la ubicación de potenciales centros de falla de las redes. Tal como se observa en los datos provistos por la Figura 1 y la Figura 2, la similitud en clustering pero divergencia en grado promedio sugiere que las redes sociales y de infraestructura tienen mecanismos distintos de resiliencia: mientras Facebook depende de hubs, los aeropuertos parecerían redistribuir críticidad en nodos intermedios (no necesariamente los más conectados).

3.1.3. Modelos de Redes — Características Generales

Ahora bien, ¿Qué tan bien capturan los prototipos de redes las caracteristicas topológicas que sugieren estos contrastantes mecanismos de resiliencia? Para responder tal pregunta, comparamos la distribución de grado de los datasets con la de una instancia de los prototipos:



(a) Aeropuertos (log-log).



(b) Facebook (log-log).

Figura 3: Comparación de las distribuciones de grados (log-log) para Aeropuertos y Facebook vs modelos de téoricos.

Distribución de Grados

Grafo	Modelo	Clustering promedio	Distancia promedio	Grado promedio
Aeropuertos	Red Real	0.5575	3.0217	24.2696
	Erdős–Rényi	0.0172	2.6247	24.4422
	Watts–Strogatz	0.5267	3.1572	24.0000
	Barabási–Albert	0.0529	2.5558	23.7946
Facebook	Red Real	0.6055	3.6925	43.6910
	Erdős–Rényi	0.0108	2.6071	43.6019
	Watts–Strogatz	0.5375	2.9666	44.0000
	Barabási–Albert	0.0363	2.5363	41.7816

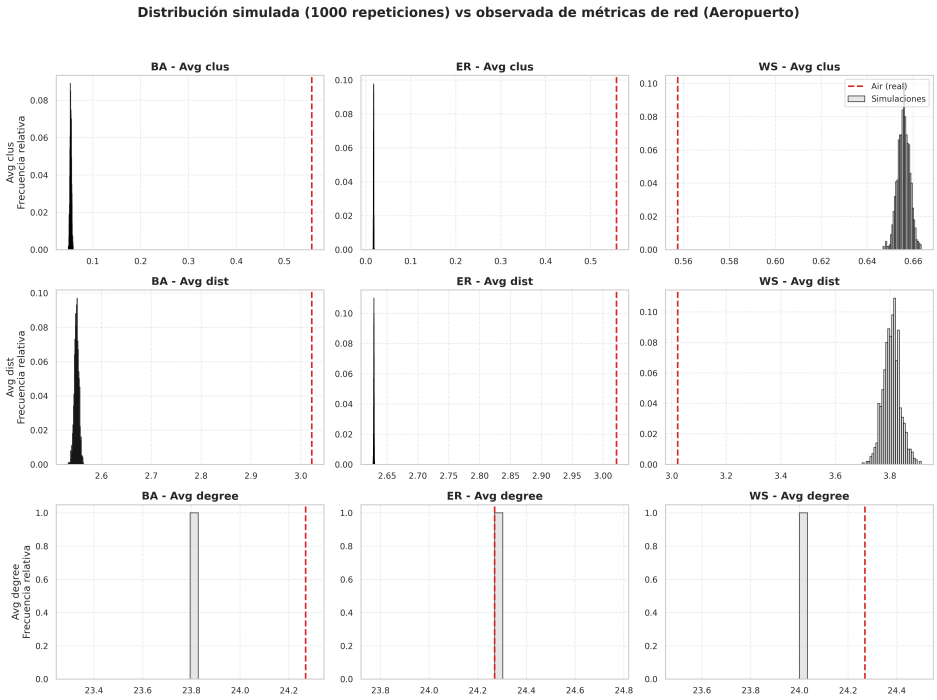
Figura 4: Métricas topológicas para las redes de Aeropuertos y Facebook, y sus modelos de referencia

Cuadro resumen de métricas topológicas comparativas

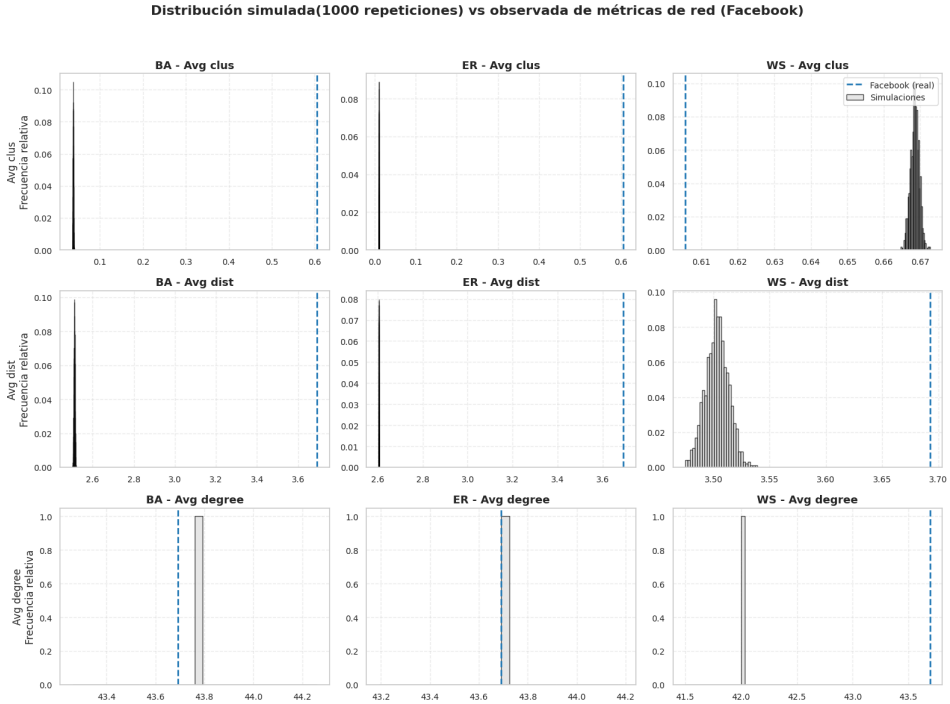
Observaciones Tal como observamos en la Figura 3 y la Figura 4, los modelos clásicos (ER, BA) no parecieran capturar la importancia estructural de nodos periféricos con alto clustering. Por su parte, la cercanía entre Watts-Strogatz y las redes reales sugiere que la resiliencia depende de estructuras locales (triángulos sociales) más que de hubs centrales. La brecha entre el clustering real (0.5575) y el predicho por Barabási-Albert (0.0529) en aeropuertos evidencia que los modelos basados en hubs subestiman la importancia de nodos periféricos con alta cohesión local.

3.1.4. Comparación de distribución simulada de métricas topológicas de los modelos prototipos de Erdős–Rényi, Watts–Strogatz y Barabási–Albert

¿Qué pasa cuando realizamos simulaciones sobre tales prototipos?



(a) Aeropuertos.



(b) Facebook.

Figura 5: Distribución simulada de métricas topológicas con 1000 repeticiones para Aeropuertos (a) y Facebook (b).

Resultados observados

Aeropuertos - Prototipos de Redes Los resultados del análisis de simulaciones para cada uno de los modelos de red (Barabási-Albert, Erdős-Rényi y Watts-Strogatz), calculando el promedio y la desviación estándar de métricas clave como el coeficiente de clustering y la distancia promedio. En todos los casos, los valores observados en la red real se ubicaron fuera del rango típico de los modelos simulados, especialmente en lo que respecta al clustering.

Este resultado sugiere que la estructura de la red de aeropuertos no es producto del azar, sino que responde a patrones específicos de organización que los modelos aleatorios no logran capturar adecuadamente. No obstante, es importante destacar que el modelo de Erdős-Rényi predice con bastante precisión el grado promedio observado en ambas redes reales.

Respecto al coeficiente de clustering, los modelos Barabási-Albert y Erdős-Rényi presentan valores promedio ± 2 desviaciones estándar que no alcanzan los niveles observados en la red real, mientras que el modelo de Watts-Strogatz es el que mejor aproxima este indicador. En cuanto a la distancia promedio, el modelo Watts-Strogatz tiende a sobreestimarla en aproximadamente 0,8 unidades, mientras que los modelos Barabási-Albert y Erdős-Rényi la subestiman en alrededor de 0,5 unidades siendo estos las mejores aproximaciones

Facebook - Prototipos de Redes La red real de Facebook presenta una estructura compleja que no logra ser replicada por completo mediante los modelos prototipo tradicionales utilizados en este análisis. Al comparar sus principales métricas con las obtenidas a partir de 1000 simulaciones de los modelos de Erdős–Rényi, Watts–Strogatz y Barabási–Albert, se observan diferencias importantes que permiten evaluar las limitaciones de cada uno.

En primer lugar, el modelo de Barabási–Albert es el único que consigue reproducir con precisión el grado promedio de la red real de Facebook. Esto se debe a que dicho modelo se basa en un mecanismo de crecimiento por adjunción preferencial, lo que genera distribuciones de grado similares a las observadas en redes reales, especialmente en aquellas con alta heterogeneidad estructural. El modelo de Erdős–Rényi también alcanza un valor cercano, aunque esto se explica por una parametrización intencional que fuerza la coincidencia del grado medio. Por otro lado, el modelo de Watts–Strogatz subestima levemente esta métrica, lo que refleja su incapacidad para generar nodos altamente conectados.

Sin embargo, cuando se analiza el clustering promedio, que refleja la tendencia de los nodos a formar grupos cerrados o comunidades locales, se evidencian limitaciones importantes. La red de Facebook presenta un alto nivel de agrupamiento, propio de las redes sociales, que no es capturado ni por el modelo de Erdős–Rényi ni por el de Barabási–Albert. Ambos generan estructuras con un clustering promedio significativamente más bajo. En cambio, el modelo de Watts–Strogatz ofrece una mejor aproximación, aunque aún por debajo del valor observado en la red real. Este resultado pone de manifiesto la dificultad de los modelos clásicos para reproducir la cohesión local típica de redes sociales complejas.

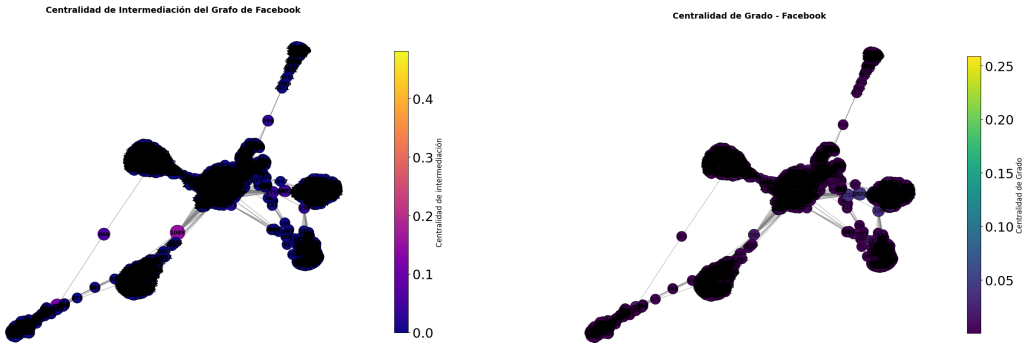
Respecto de la distancia promedio —entendida como la longitud media de los caminos más cortos entre pares de nodos—, la red real exhibe una estructura eficiente, característica de las llamadas redes “small-world”. El modelo de Watts–Strogatz logra aproximarse razonablemente a este comportamiento, mientras que el modelo de Erdős–Rényi presenta distancias demasiado reducidas y el de Barabási–Albert, distancias excesivamente bajas. Estos resultados muestran que, aunque el modelo WS no replica fielmente todas las métricas, sí consigue reflejar de forma más equilibrada la eficiencia estructural observada en la red.

En conjunto, los resultados sugieren que ningún modelo logra reproducir de manera integral las propiedades clave de la red de Facebook. Mientras que Barabási–Albert reproduce con precisión el grado promedio, falla en capturar la cohesión local. Watts–Strogatz, en cambio, se aproxima mejor al clustering y a la distancia promedio, pero subestima el grado. Esto evidencia las limitaciones de los modelos prototipo clásicos para representar adecuadamente la complejidad estructural de redes sociales reales, y refuerza la necesidad de explorar enfoques más flexibles o híbridos que integren múltiples mecanismos de formación de enlaces.

3.2. Centralidades

En el marco de la hipótesis planteada, resulta relevante primero clasificar los nodos según alguna medida de centralidad que nos permita, por un lado caracterizar a las redes, y por otro, ejecutar nuestras dos estrategias de ataque. Con este objetivo, cuantificamos y caracterizamos estos nodos para comprender su relevancia dentro de la estructura de la red. Para ejecutar nuestras estrategias de ataque, consideramos que utilizar la centralidad de grado como criterio para definir y medir la importancia de los hubs. De manera adicional, calculamos otros tipos de centralidades (como intermediación) con el objetivo de caracterizar a las redes previo a la ejecución de las simulaciones. A fin de facilitar el análisis de tales caracterizaciones, se construyeron los gráficos 6a, 6b, 8b y 8a de las redes de Aeropuertos y Facebook.

3.2.1. Comparación de Centralidad de Intermediación y Grado - Facebook



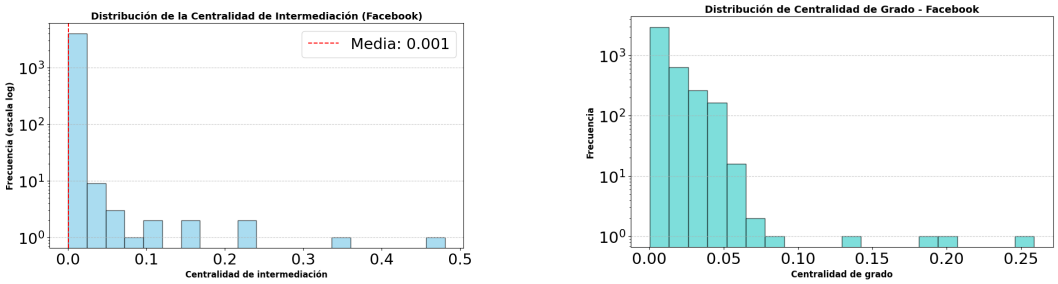
(a) Centralidad de Intermediación - Facebook

(b) Centralidad de Grado - Facebook

Figura 6: Comparación Centralidad de Grado entre (a) Aeropuerto y (b) Facebook.

Como puede observarse en las figuras 6a y 6b, la estructura de la red analizada presenta comunidades más compactas y claramente delimitadas, lo que sugiere una organización interna caracterizada por altos niveles de cohesión entre los nodos de cada grupo. Asimismo, se evidencia un patrón estructural variable y de carácter aleatorio, lo cual indica la ausencia de una distribución fija o predecible en las conexiones entre los elementos de la red.

En la figura correspondiente a la centralidad de grado, se identifican los hubs o influencers, es decir, aquellos nodos con un alto número de conexiones directas. Por otro lado, en la figura de centralidad de intermediación se destacan aquellos nodos que, aunque no necesariamente sean influencers, desempeñan un papel crucial en el flujo de información al actuar como puentes entre distintas partes de la red, facilitando su propagación a través de toda la estructura.



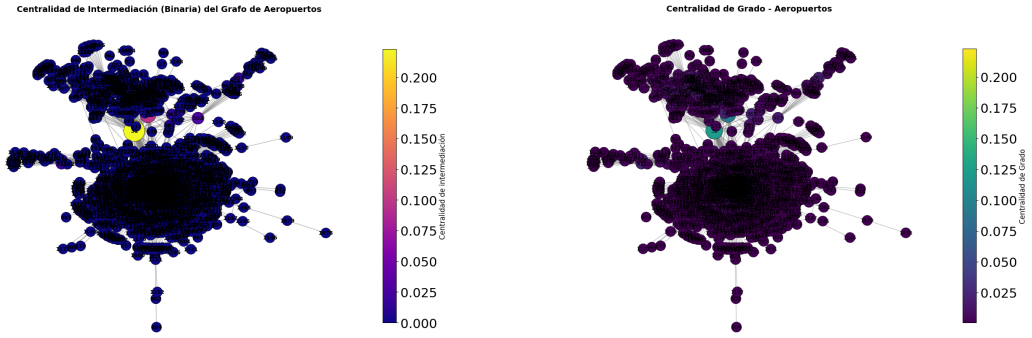
(a) Distribución de centralidad de intermediación del grafo de Facebook

(b) Distribución de centralidad de Grado del grafo de Facebook

Figura 7: Distribución de centralidad de intermediación y Grado

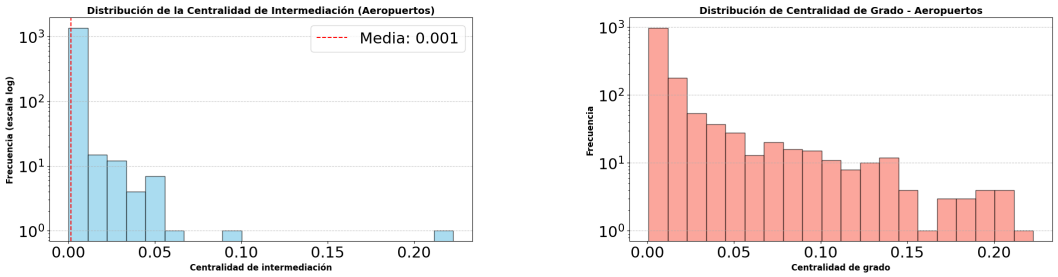
Otro aspecto relevante que puede observarse las figuras 7a y 7b es la presencia de hubs, representados principalmente por los influencers, quienes actúan como nodos centrales con un alto grado de conexión y desempeñan un papel clave en la difusión de información dentro de la red.

3.2.2. Comparación de Centralidad de Intermediación y Grado - Aeropuertos



(a) Centralidad de Intermediación (b) Centralidad de Grado

Figura 8: Comparación entre Centralidad de Intermediación (a) y Centralidad de Grado (b) en la red de aeropuertos.

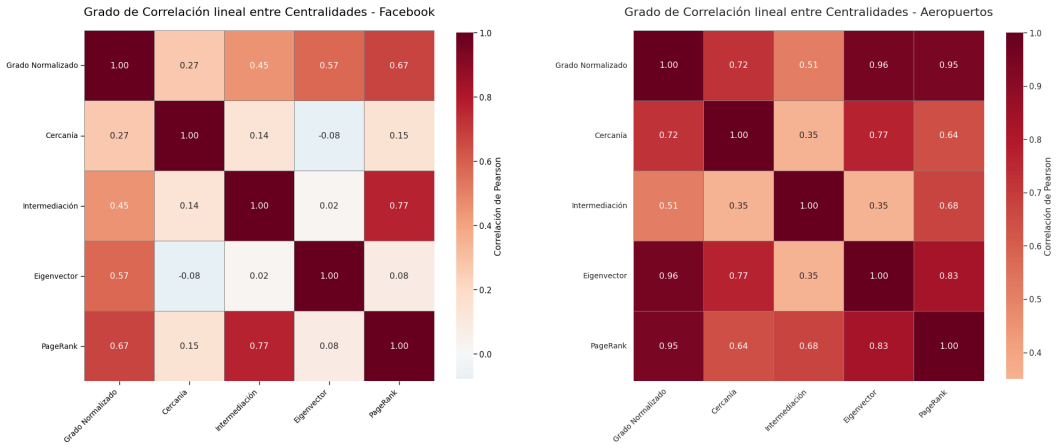


(a) Distribución de centralidad de intermediación (b) Distribución de centralidad de Grado

Figura 9: Distribución de centralidad de intermediación (a) y Distribución de centralidad de Grado (b)

En la visualización de la centralidad de grado de la red de aeropuertos, se observa que algunos nodos con alta centralidad, coloreados en verde, se destacan por ser ciertos aeropuertos ubicados en zonas periféricas, como los que conectan con el interior de una ciudad. Esta visualización permite identificar rápidamente su rol estratégico como nodos de escala obligada para acceder a regiones con menor conectividad directa. Dichos aeropuertos actúan como puntos clave de enlace, a pesar de estar geográficamente aislados.

3.2.3. Correlación lineal entre centralidades



(a) Heatmap de Correlación entre centralidades - Facebook

(b) Heatmap de Correlación entre centralidades - Aeropuertos

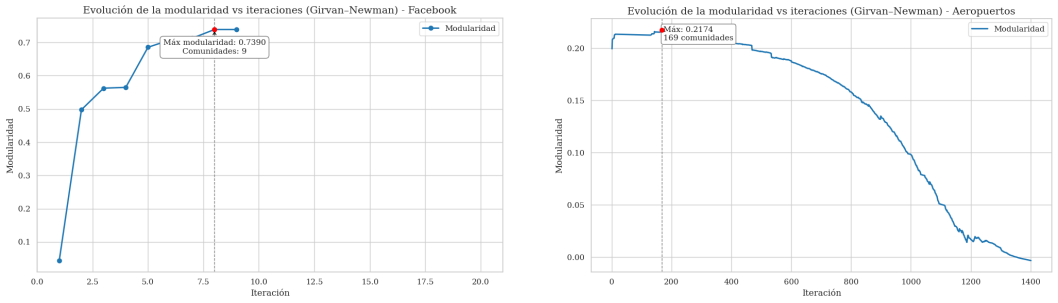
Figura 10: Grado de Correlación lineal entre Centralidades

Del análisis del grado de correlación lineal entre las centralidades de las redes bajo estudio, que se presentan en las figuras 10a y 10b, se observa que los aeropuertos con mayor número de conexiones directas (grado) también tienden a ser globalmente relevantes según las medidas de Eigenvector y PageRank, con correlaciones de 0.96 y 0.95, respectivamente. Esto indica que los hubs más grandes no solo concentran rutas, sino que están conectados con otros aeropuertos importantes dentro de la red. Por otro lado, la intermediación exhibe una dinámica distinta: sus correlaciones más bajas con Grado (0.51), Eigenvector (0.35) y PageRank (0.67) indican que resalta aeropuertos que, aunque menos conectados, desempeñan un rol estratégico como puentes entre regiones o zonas periféricas. Estos resultados parecen mostrar una estructura dual en la red de aeropuertos, donde coexisten grandes centros de tráfico con nodos clave que garantizan la conectividad entre distintas partes del sistema.

En la red de Facebook, las centralidades muestran correlaciones lineales en su mayoría moderadas o bajas. Grado se relaciona con PageRank (0.67) y Eigenvector (0.57), pero menos con Intermediación (0.45) y Cercanía (0.27). Intermediación tiene una alta correlación solo con PageRank (0.77), y Eigenvector apenas se relaciona con otras medidas (por ejemplo, –0.08 con Cercanía y 0.02 con Intermediación). Este patrón indica que la red no concentra su estructura en pocos nodos dominantes, sino que diferentes actores cumplen roles distintos: conectividad, influencia estructural o intermediación, reflejando una red más distribuida y funcionalmente diversa.

3.2.4. Comunidades.

Los gráficos en las figuras 11b y 11a muestran la evolución de la modularidad a lo largo de las iteraciones para ambas redes durante la ejecución del algoritmo. Realizamos esto con el fin de encontrar el número óptimo de comunidades con el algoritmo de Girvan-Newman, el cual se obtiene del máximo de modularidad en proceso de iteraciones. En base a los resultados realizamos las visualizaciones subsiguientes.

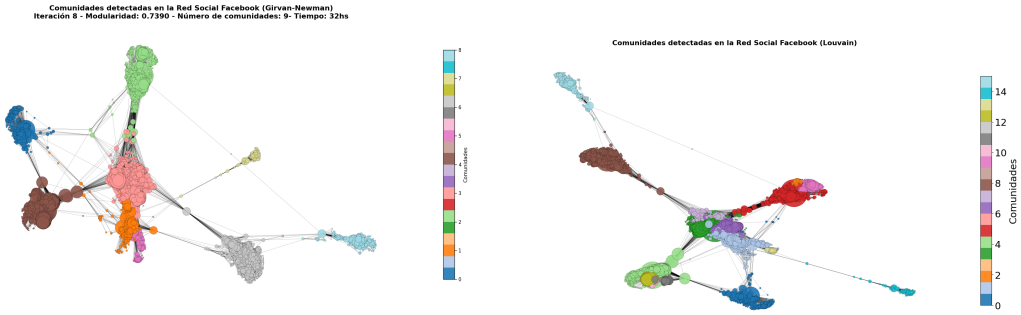


(a) Facebook - Modularidad vs Iteraciones

(b) Aeropuertos - Modularidad vs Iteraciones

Figura 11: Modularidad vs Iteraciones para las redes de Facebook y Aeropuertos

3.2.5. Comunidades detectadas para la red social Facebook por los métodos de Louvain y Girvan-Newman



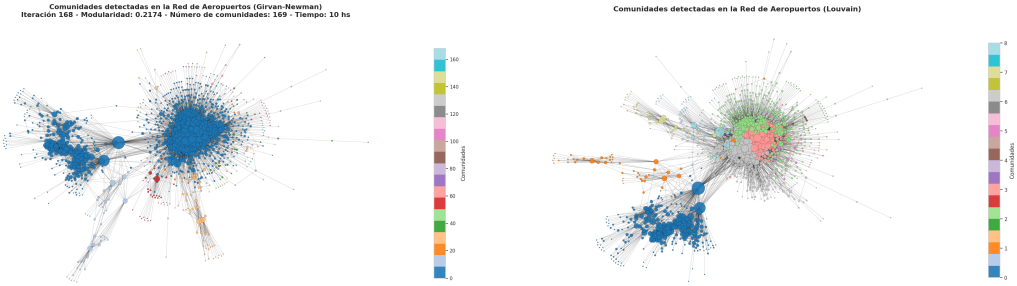
(a) Facebook - Comunidades por método de Girvan-Newman

(b) Facebook - Comunidades por método de Louvain

Figura 12: Comunidades detectadas en la red de Facebook utilizando los métodos de Girvan-Newman y Louvain

Tal como podríamos esperar en una red social, ambos métodos detectan comunidades bastante densas y separadas entre sí. Sin embargo: En Girvan-Newman, observamos menos comunidades (9) y más claramente separadas.En Louvain, hay una mayor cantidad de comunidades (15), algunas más pequeñas o subdivisiones más finas. Esto sugiere una estructura modular jerárquica, donde ciertas regiones están muy densamente conectadas internamente pero débilmente conectadas con el resto de la red. Los pocos nodos que conectan distintas comunidades (puentes entre clusters) juegan un rol clave en la conectividad global. En el método Girvan-Newman, estas conexiones son más visibles debido a cómo elimina aristas de mayor centralidad. Podríamos esperar que si se atacan específicamente estos nodos puente, se pueda fragmentar la red rápidamente, aunque estos nodos no necesariamente tengan el mayor grado. Esto tiene implicancias para nuestra estrategia de çuriosidad", pues podríamos encontrar en tales nodos (posiblemente priorizados por el sesgo curioso), alguna vulnerabilidad de bajo grado que termine causando una disrupción sistemica. Ahora bien, dicha estrategia, si bien podría proveernos de información útil en torno a la detección de anomalias, no esperamos que sea más efectiva que atacar nodos de alta centralidad de grado. En el dataset de Facebook, como hay hubs conectando muchas comunidades, removerlos puede causar disrupciones sistémicas (desconectar grandes partes de la red).

3.2.6. Comunidades detectadas para la red de Aeropuertos por los métodos de Louvain y Girvan-Newman



(a) Girvan-Newman (b) Louvain

Figura 13: Comunidades detectadas en la red de aeropuertos utilizando los métodos de Girvan-Newman y Louvain.

Girvan–Newman sugiere una red muy vulnerable a estrategías dirigidas dado a que pocos nodos conectan grandes sectores de la red (centralización) por lo que eliminar un hub podría fragmentar la red fuertemente. Ahora bien, Louvain, al identificar más comunidades pequeñas, reduce esta vulnerabilidad. Parecería existir más redundancia estructural. A lo que respecta a ataques aleatorios con sesgo a nodos periféricos (baja centralidad), estos ataques suelen tener menor impacto en ambas configuraciones. La gran comunidad de Girvan–Newman es más robusta a ataques aleatorios porque muchos nodos son hojas o tienen poca conectividad local. Por su parte, Louvain, al tener más comunidades pequeñas, podría ver efectos localizados, pero no una desconexión masiva. Quedaría preguntarnos si a pesar.

La aplicación del algoritmo Louvain sobre la red de aeropuertos permitió detectar ocho comunidades distintas, representadas con colores únicos en el grafo. Esta segmentación revela agrupamientos internos densamente conectados y con menor vinculación entre sí, una característica típica de redes con estructura modular.

En el grafo visualizado, puede observarse cómo ciertas comunidades —como la naranja y la verde— concentran una gran cantidad de nodos y presentan conexiones más intensas al interior del grupo. La representación visual, al usar color y tamaño de nodo, facilita la identificación de nodos centrales en cada comunidad y permite distinguir regiones periféricas.

Esta representación complementa el mapa geográfico mostrado anteriormente, ya que permite apreciar la estructura topológica de las comunidades independientemente de su localización espacial, reafirmando la existencia de módulos coherentes dentro de la red.

3.2.7. Comparación de Comunidades de la red de Aeropuertos y Facebook

Cuadro 3: Comparativa entre algoritmos de detección de comunidades en la red Facebook

Métrica	**Girvan–Newman**	**Louvain**
Número de comunidades	9	16
Modularidad	0.7390	0.835
Tamaño máx. comunidad	926 nodos	548 nodos
Tamaño mín. comunidad	60 nodos	19 nodos
Tiempo de ejecución	32 horas	30 minutos

Cuadro 4: Comparativa entre algoritmos de detección de comunidades en la red de Aeropuertos

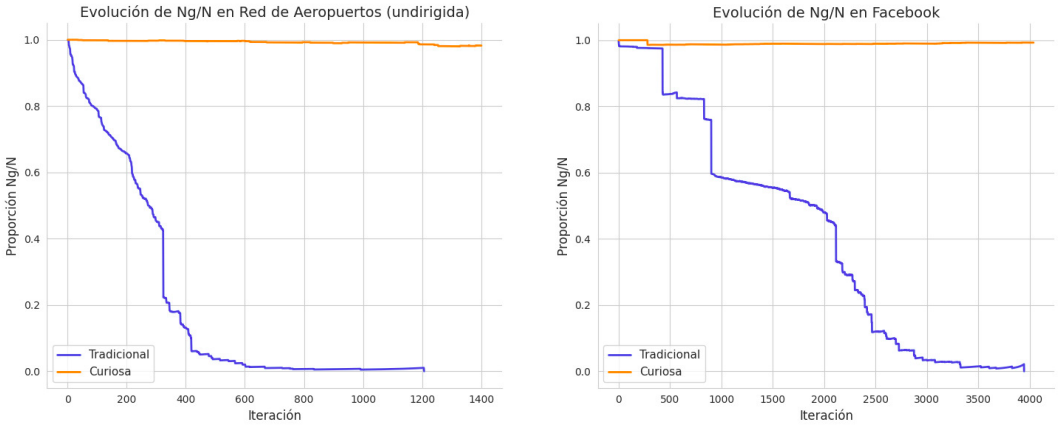
Métrica	**Girvan–Newman**	**Louvain**
Número de comunidades	169	8
Modularidad	0.2174	0.3479
Tamaño máx. comunidad	785 nodos	432 nodos
Tamaño mín. comunidad	1 nodo	4 nodos
Tiempo de ejecución	10 horas	15 minutos

En el análisis comparativo de redes, se observa que Facebook presenta una estructura con patrones más aleatorios, en contraste con la red de aeropuertos, cuyo diseño responde a una planificación previa e implica el desarrollo de una infraestructura física concreta. Esta diferencia marca una separación clara entre una red de origen orgánico, como Facebook, y otra construida sobre criterios logísticos y geográficos, como la de los aeropuertos.

Dentro de la red de aeropuertos, al examinar comunidades con pocos nodos —por ejemplo, grupos formados por entre 1 y 4 nodos dentro del grafo— se identifican ciertos aeropuertos ubicados en zonas periféricas que adquieren un rol destacado. A pesar de su baja conectividad, estos aeropuertos actúan como puntos de enlace entre nodos aislados y el interior de la ciudad, cumpliendo así una función de conectores críticos dentro de la red.

Este tipo de estructura podría tener implicancias importantes para estrategias basadas en la curiosidad estructural, ya que estos aeropuertos periféricos —que a simple vista podrían parecer irrelevantes— pueden en realidad representar vulnerabilidades anómalas. Su posición intermedia y su capacidad de conexión limitada los convierten en puntos potencialmente frágiles, cuya identificación resulta clave para comprender la dinámica de la red y anticipar fallos.

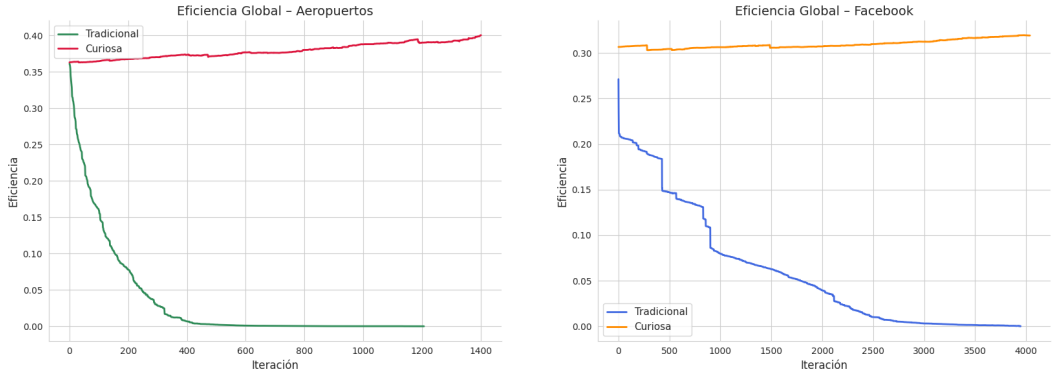
3.3. Experimentos de robustez



(a) Aeropuertos (b) Facebook

Figura 14: Resultados del experimento para redes de aeropuertos y Facebook

Contrariamente a lo que podiamos esperar dado nuestro analisis explotario preliminar, la estategia de curiosidad no provee disrupciones a ninguna de las dos redes, ni siquiera a la de Aeropuertos. En la estrategia de ataque de curiosidad, el tamaño relativo de la componente gigante resultante se observa estable en ambas redes. Esto nos indica que durante ese recorrido iterativo no se dectectó ninguna anomalía disruptiva. Si bien cada red tiene un decaimiento de conectividad con particularidades, con la estrategia Tradicional (azul), el componente gigante se reduce rápidamente en ambos casos: basta eliminar unos cientos de nodos para desconectar gran parte de la red. Ambas redes terminan siendo vulnerables a ataques dirigidos aunque en la red de Aeropuertos existe un decaimiento de la red progresivo mientras que en Facebook esto se da de saltos. Esto es esperado dada la topología hub-dependiente y libre de escala de la red de Facebook la cuál termina siendo más susceptible a ataques dirgidos. Tal como remarcamos previamente, con la estrategia Curiosa (naranja), la red se mantiene conectada casi completamente. Esto indica que eliminar nodos poco centrales no afecta la conectividad estructural, por lo que amnas redes resultaron altamente robustas ante fallos aleatorios sesgados hacía nodos marginales.



(a) Aeropuertos (b) Facebook

Figura 15: Resultados del experimento para redes de aeropuertos y Facebook

En refuerzo a lo descubierto al observar el tamaño relativo de la componente gigante, las medidas de Eficiencias Global simplemente reflejan la misma realidad: ambas redes se mostraron resilientes a tales ataques, no solo su eficiencia global no decayó sino que se incrementó progresivamente.

4. Conclusión

En el contexto de redes cada vez más complejas y enriquecidas, y un creciente interés por explorar estrategias alternativas para detectar riesgos sistémicos y vulnerabilidades no convencionales basadas en curiosidad computacional, este informe contribuyó a esclarecer la efectividad de dichas alternativas de ataque en dos redes de topologías marcadamente contrastantes. En tanto nuestro análisis exploratorio preliminar nos sugirió que al menos una de las redes (Aeropuertos) podría ser más vulnerable a ataques atípicos dada su mayor heterogeniedad, menor clusterización y mayor conectividad, al implementar ambas estrategias de ataque observamos que sistemáticamente aquellas que priorizan progresivamente nodos de mayor centralidad de grado son aquellas que terminan disrumpiendo la red. Si bien si esperábamos una mayor eficiencia general de la estrategia tradicional, la estrategia curiosa tampoco resultó ser efectiva para revelar "vulnerabilidades ocultas"puesto que las caídas de eficiencia y conectividad solo se presentaban en las últimas iteraciones de la simulación. En otras palabras, para que la estrategia de curiosidad cause alguna disrupción se debía iterar hasta borrar casi todos los enlaces de los nodos. Esto nos indica, por un lado, que esos nodos omitidos al final eran, en efecto, cruciales y por otro, que ningún nodo "no evidente"terminó causando alguna disrupción inesperada o anomala. Futuras investigaciones podrían contemplar otras medidas de centralidad de grado, estrategias con una mayor complejidad para cada iteración (contemplar grado e intermediación en el marco de ciclos), o incluso experimentar con distintos factores de peso para el sesgo de curiosidad.

Referencias

[1] Freitas, S., Yang, D., Kumar, S., Tong, H., & Chau, D. H. (2022). Graph vulnerability and robustness: A survey. *IEEE Transactions on Knowledge and Data Engineering, 35*(6), 5915–5934. `https://arxiv.org/pdf/2105.00419`

[2] Zanartu, F., Treude, C., & Wagner, M. (2023). Socialz: Multi-Feature Social Fuzz Testing. *arXiv preprint* arXiv:2302.08664. `https://dl.acm.org/doi/pdf/10.1145/3638529.3654033`

[3] Zanartu, F., Treude, C., & Wagner, M. (2023). Socialz: Multi-Feature Social Fuzz Testing. *arXiv preprint* arXiv:2302.08664.

[4] Furno, A., El Faouzi, N.-E., Sharma, R., & Zimeo, E. (2021). Graph-based ahead monitoring of vulnerabilities in large dynamic transportation networks. *PLoS ONE, 16*(3), e0248764.

[5] Li, Y., Chen, Z., Zha, D., Zhou, K., Jin, H., Chen, H., & Hu, X. (2020). AutoOD: Automated Outlier Detection via Curiosity-Guided Search and Self-Imitation Learning. *arXiv preprint* arXiv:2006.11321.

[6] Cai, X., Cui, Z., Bai, X., Ke, R., Ma, Z., Yu, H., & Ren, Y. (2024). VCAT: Vulnerability-aware and Curiosity-driven Adversarial Training for Enhancing Autonomous Vehicle Robustness. *arXiv preprint* arXiv:2409.12997.