

Resilience of Ghost Company Networks in Ecuador: A Computational Forensic Audit Framework

Xavier Torres-Maldonado^{1,*}, Carlos Redroban-Ortiz², Lissete Reyes-Vanegas³ and Xavier Mosquera-Rodríguez²

¹Universidad Central del Ecuador, Pichincha, Ecuador

²Universidad ECOTEC, Samborondon, Ecuador

³Universidad Espíritu Santo, Samborondon, Ecuador

Abstract

In the Big Data era public sector auditing needs to change the way it works to keep up with the ways companies cheat. This paper shows a way to use computer intelligence to find the structure of ghost companies in Ecuador by combining auditing with looking at complex networks. A repeatable method was developed using Python that keeps data private through SHA-256 hashing, which facilitates a deep understanding of the situation by applying concepts from network science. The results show that the system of cheating is very organized and connected in a way. When we tested what would happen if we targeted parts of the system, we found out that if we take out 72 key points the whole system falls apart, which means that we do not need to fix everything, just the important parts. The Big Data era and public sector auditing are important here. The findings from this study give people in charge a tool to move from just watching what happens to actually being, in control. Public sector auditing and the Big Data era are connected in this way.

Keywords

Forensic Auditing, Complex Networks, Python workflow, Data Resilience, Public Control

1. Introduction

Fiscal integrity and government control oversight in Ecuador have used methods for a long time. These methods are based on checking documents one by one. This way of doing things is based on administrative inspection. It assumes that financial problems are easy to find in transactions [1, 2]. However, companies are becoming more complex. They are like networks that make it hard to know who really owns them. Because of this the usual ways of auditing are not working well. They are missing a lot of information [3].

This is happening because people who do not pay taxes and are involved in financial activities are getting smarter. They are staying one step of the people who are supposed to be in control. The people in charge are using methods that are not changing but the people doing bad things are always adapting and finding new ways to do them. Fiscal integrity and public procurement oversight, in Ecuador are having a time keeping up with this [4, 5].

To tackle these evasion plans we suggest a fresh method based on Structural Intelligence. This approach uses network science to analyze government databases. Think graph theory and network metrics [6, 7]. Unlike systems that look at firms separately, the method sees the states financial system as a whole. It understands that risk doesn't come from one transaction but from where each player stands in the network [8, 9, 10]. We look at the state ecosystem as a complex system. Risk comes from the position of each actor in the network. This is not about one transaction. It is about how everything connects.

ICAIW 2026: Workshops at the 9th International Conference on Applied Informatics 2026, October 13–17, 2026, Orlando, United States

*Corresponding author.

✉ xmtorres@uce.edu.ec (X. Torres-Maldonado); credrobano@ecotec.edu.ec (C. Redroban-Ortiz); lissete.reyes@uees.edu.ec (L. Reyes-Vanegas); xmosquera@ecotec.edu.ec (X. Mosquera-Rodríguez)

🆔 0009-0003-5338-0449 (X. Torres-Maldonado); 0000-0002-0672-5323 (C. Redroban-Ortiz); 0000-0002-1363-3443 (L. Reyes-Vanegas); 0000-0003-1810-3887 (X. Mosquera-Rodríguez)



© 2026 Copyright for this paper by its authors. Use permitted under Creative Commons License Attribution 4.0 International (CC BY 4.0).

The broken way of moving from pyramid-shaped structures to a flat, web-like setup needs a big change from checking after things happen based on what has already been found to stopping problems before they start [11, 12]; this change is not just about technology; it is very important for society to restore agreement between people [13, 14]. As noted by Chen and Neshkova [8], using kinds of graph neural networks and methods to find groups in data helps spot secret deals that people or basic computer programs can't see with math.

This paper provides the implementation of a technical system, covering the full pipeline from data preprocessing to fluid simulation, by using determinant hashing (SHA-256) for privacy-preserving analysis. We address the legal imperatives of the *Ley Orgánica de Protección de Datos Personales* while maintaining topological accuracy [15]. Furthermore, we introduce the RODES model (Role, Objective, Data, Expectation, Structure) to guide AI-assisted interrogation of complex datasets, democratizing the use of advanced analytics within audit institutions [16, 17, 18].

This study demonstrates that fraudulent networks in Ecuador exhibit a clear scale-free topology [19, 20], where a small number of hubs maintain system connectivity despite environmental disruptions, quantifying the modularity index (Q) [21, 22]. Demonstrates that these networks are deliberately engineered to be compartmentalized, thereby minimizing risk contagion between illicit cells; consequently, this study offers compelling arguments for Supreme Audit Institutions (SAIs) to implement data-driven control, fostering the development of technical skills among auditors-moving them from manual verification to proactive structural disruption [23, 24, 25].

This research shows that forensic auditing can really make a difference when it is guided by data. The forensic workflow that uses Python and is presented here can be used by national or regional control bodies. This will help the fight against corruption to keep up with the changes in the economy that are happening because of technology. Forensic auditing is a tool in this fight, and the Python-based forensic workflow is a big part of it. Forensic auditing and the Python-based forensic workflow can help make sure that corruption does not get ahead of us [26, 27, 28].

2. Theoretical Framework

2.1. The Topology of Illicit Networks

Fraudulent networks in Ecuador do not just happen; they have a complicated system. This system is like a web. It has important points that hold everything together. These points are connected to a lot of points; these points are not random. It follows a pattern where a few points are very important. The rest of the points are connected to these ones. This is what makes the whole system work. Fraudulent networks in Ecuador have this kind of system. It is like a network, with a few important points that hold everything together [19, 20].

These illicit networks are really strong because of how they're organized not because they are big. The way they are set up in a hierarchy is what helps them to keep their activity separate [29, 30]. This setup is special because the important parts of the network the parts that're really well connected tend to connect with each other. This forms a kind of core and outer layer. It is hard for regular audit methods to get through to the core of these illicit networks. The illicit networks have a lot of links, between the parts, which makes them even stronger. The way the illicit networks are organized is what makes it so hard to catch the people who are doing the activity [21, 22].

This kind of network setup has consequences for how it works. It helps keep dealings separate on purpose. We can measure this separation using something called the modularity index, or (Q) for short [31, 22]. In Ecuadors networks of shell companies a high (Q) value, close to 1.0, means the network is split into groups that are tightly connected within but not much outside. Each of these groups or communities has some independence [32].

This way of organizing things has risks. If one part of the network gets caught or discovered by authorities the damage mostly stays in that one part. It does not spread to the organization. Shell company networks still use this method. The compartmentalization strategy contains risk since if one cell of the company network is compromised or detected by control authorities the resulting exposure

remains largely confined to that cell of the shell company network rather than spreading to the entire organization of shell companies.

This is a compartmentalization, a property that can be measured empirically through the modularity index of community structures in shell company networks. In Ecuador's shell-company networks, a Q-value, close to 1.0 indicates that the shell company network is divided into dense internally cohesive subgraphs or communities, each with a certain degree of autonomy, in Ecuador's shell-company networks [33, 20].

Researchers have found out that these groups of criminals also take advantage of something called the "small-world" network. This means that the distance between any two companies is really small. They can move money and assets around quickly because the paths between these companies are short. This helps them move assets across many different countries with different tax laws. There are also people who help make this happen like accountants, shareholders or lawyers who work with these companies a lot. These people are, like connectors that bring together companies that would not normally be connected to each other [32, 34, 28].

These networks can also change. If you take away a node that's not really important it does not affect the whole system's ability to move illegal money. This is because the system can replace the node that was removed quickly [12, 20]. Understanding how strong the system is is really important. The reason is that the system is weak in a group of central nodes. These central nodes are the people who come up with the fraud. If you can find out who they are and remove them it can cause the whole illegal system to fail [6, 35].

2.2. Forensic Auditing and Digital Transformation

The digital transformation of Supreme Audit Institutions (SAIs) is not simply a matter of adopting new software, it represents a fundamental shift in how we think about financial oversight. As financial transactions increasingly move online, auditors can no longer rely solely on manual reviews of accounting records. This traditional approach is too slow to keep pace with the speed at which more moves today. In this sense, digital transformation is reshaping the very foundations of how Supreme Audit Institutions exercise control over public funds.

Auditors have to go beyond number crunching. They need to look at how things are connected in digital economies; they must follow the Ley Orgánica de la Contraloría General del Estado (LOCGE) rules [2, 23]. To do those auditors changes how they work, they need to use tools to oversee things quickly and effectively. This will help keep institutions honest in areas where cybercrimes happen often [25]. These areas are called cyber environments. Auditors need to safeguard institutions in these environments. They must make sure everything is okay with money and taxes. The (LOCGE) rules are important here.

Bringing forensic science to the public sector is a big change. It means we need to be better at dealing with cyber threats. We have to be able to find fraud by looking at a lot of kinds of information very quickly. The United States GAO has done audits that show that when the way we do audits changes fast as the technology around us the institutions get better at handling problems [25].

This is very important in Ecuador. The people who do audits have to be like detectives. They have to be able to follow the money and see where it goes by looking at clues on computers rather than just checking invoices. Digital forensic science is a part of this. The people who do audits need to understand forensic science to do their jobs well. They need to be able to use forensic science to help them find fraud and make sure the public sector is working correctly [2].

Recent studies show that technology is now a part of modern auditing. It is not something extra, but it is the main way that people try to stop others from cheating on their taxes. There are tools that can check a lot of information at the same time. These tools can look at what people buy and sell and also check information about them. This helps the people in charge of checking for tax cheating to do their job better and be more open about what they do [26, 35, 24].

This change is also helping to make it harder for people to hide the truth about who owns companies. This is a problem when it comes to stopping money laundering. As companies get more complicated,

the people who check for tax cheating have to get smarter. If they do not, then the bad people will find ways to cheat by using loopholes in the tax laws of countries [36, 37, 27].

The digital transformation of auditing is really important for making a big difference in the fight against corruption [38]. Using Python to analyze data and automating work helps the people in charge stay on top of things as the economy becomes more digital [39]. This means we are using technology, law, and forensic science together to create a way of governing that is based on data and can be trusted by the public. The digital transformation of auditing is the key to all of this. It helps us make sure that we are following the rules and that people trust the government. The digital transformation of auditing is what makes this all possible [35, 24].

3. Methodology

The way we do things in this framework is pretty straightforward. We follow a three-step process. This process is designed to work for small tasks. We can repeat it many times, and it will always follow the rules about keeping data private. The Ecuadorian ISAI gets information from this process. We use Topological Intelligence and prompt engineering to turn transaction data into something the CGE can actually use and use this information to make decisions.

The data analyzed were obtained from the public registry of ghost companies maintained by Ecuador's Internal Revenue Service (SRI) (<https://www.sri.gob.ec/empresas-fantasma>), as of January 31, 2026. The full network comprised 3,588 nodes and 5,284 links. The analysis, however, focuses on the resilience of individual components — starting with the largest, made up of 341 nodes — since each component represents a group of interconnected companies operating independently of the other groups within this ecosystem of tax fraud and corruption.

3.1. Privacy-Preserving Data Workflow

To comply with the *Ley Orgánica de Protección de Datos Personales*, the workflow applies deterministic hashing rather than conventional anonymization. SHA-256 keeps the network's topological properties (its links) intact, enabling structural mapping (seeing which nodes are connected to one another) without revealing the underlying identity of the corporate entities involved [15].

Script 1: Secure Data Ingestion

```
Python
import hashlib
import pandas as pd
def process_anonymization(df, identifier_col):

    df['node_id'] = df[identifier_col].apply(
        lambda x: hashlib.sha256(str(x).encode()).hexdigest()
    )
    return df
```

3.2. Structural Modeling and Modularity Analysis

The model of the network is an undirected graph $G = (V, E)$, where V represents companies and E represents shared structural, commercial, or financial ties. To assess the resilience of these structures, we compute Betweenness Centrality (C_B), which identifies the brokerage roles that are critical to the network's overall integrity [21, 40].

Script 2: Network Centrality and Community Detection

```
Python
```

```
import networkx as nx
from networkx.algorithms.community import louvain_communities
def characterize_network(G):
    centrality = nx.betweenness_centrality(G)
    communities = louvain_communities(G)
    return centrality, communities
```

3.3. AI-Assisted Auditing: The RODES Model

To connect complex network theory with forensic practice, we introduce the RODES model [18], a framework that standardizes the interaction between the auditor and the Large Language Model (LLM). RODES ensures that the model's output is consistent, technically accurate, and formatted and ready for direct import into forensic software such as Cytoscape or Gephi.

The RODES model rests on five pillars adapted to audit-specific prompt engineering:

- **Role (R):** The model adopts the persona of a forensic data scientist specialized in Ecuadorian fiscal law, keeping tone and methodology aligned with SAI standards [2, 23].
- **Objective (O):** Sets a clear detection target (risk clusters), and in particular nodes that function as bridges between distinct tax zones [17, 25].
- **Data (D):** Restricts the model to working exclusively with pre-anonymized financial ledgers, preventing accidental exposure of sensitive personally identifiable information [15].
- **Expectation (E):** Requires the output to take the form of risk-scored node lists, ranked according to the highest degree and betweenness metrics [16, 25].
- **Structure (S):** Restricts output to JSON or CSV formats, machine-readable and ready to feed directly into the resilience simulations described in the previous section [34].

The RODES integration changes the audit process from a technical task to a careful plan that is focused on public policy. Using RODES, auditors can find the 72 points that are part of the surgical audit strategy without needing to know a lot about graph theory [4, 8, 28, 18]. This combination of human detective work and automated analysis is a development in public control. The RODES integration is important for policy. With the RODES integration, auditors can do their job better. The audit process is not about technology; it is about public policy, and the RODES integration helps with that [24, 10].

This way of doing things wants to make Ecuadorian government offices a lot stronger so they can fight against ghost companies. It also wants to stop people from taking control of the government in a way. It wants to make sure Ecuador's rules against corruption are as good as the best ones in South America [41, 42, 11].

4. Results and Discussion

Empirical analysis shows that the corporate network is highly fragmented but still connected; it is an ecosystem designed for tax evasion. The modularity index Q equals 0.980 confirms that there are fraudulent cells with limited visibility into each other.

The simulation in Figure 1 shows that the system's integrity is fragile when targeted changes are made to its structure; the corporate network has cells that're good at hiding from each other. This makes the overall system weak to attacks. The cells in the network are designed for fiscal evasion. They do not connect much with other cells, so when we target and change some parts of the system, it can easily break.

The resilience collapse curve tells us something about the fraudulent ecosystem. If we use Betweenness Centrality to find and fix problems in the ecosystem, it can cause the system to collapse.

The fraudulent ecosystem has 72 nodes that are very important; if we remove these 72 nodes from the fraudulent ecosystem, the main part of the network gets a lot smaller.

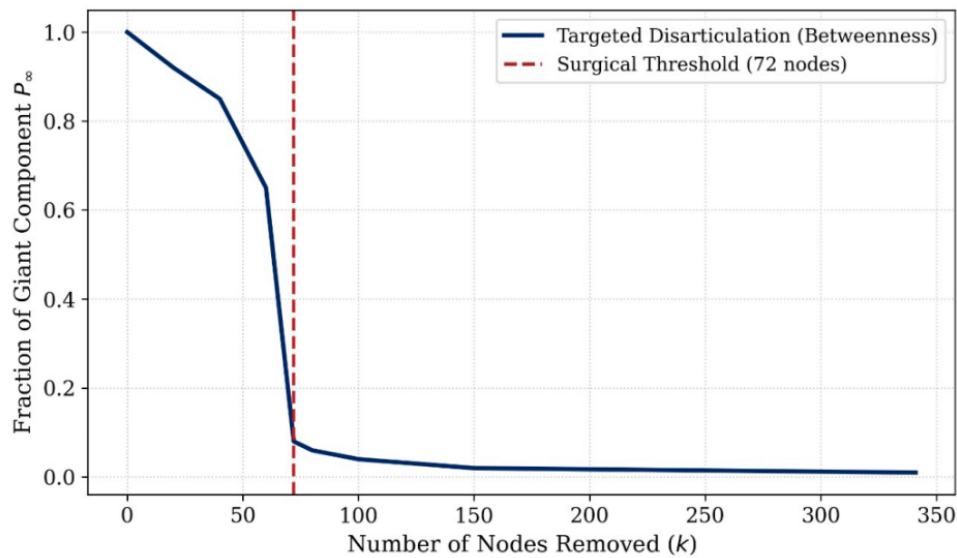


Figure 1: Network Resilience and Structural Disarticulation.

It goes from having 341 nodes to 25 nodes in the fraudulent ecosystem this is a drop of 92.6% in how well the fraudulent ecosystem works.

This result shows us that the fraudulent ecosystem is not strong like a hydra with heads; the fraudulent ecosystem actually relies on a number of important connections to work.

The resilience collapse curve and the plan to check and fix problems using Betweenness Centrality help us see this about the ecosystem.

The resilience collapse curve and Betweenness Centrality show that the fraudulent ecosystem is not as powerful as it seems to be.

The fraudulent ecosystem is actually a system that can be weakened by removing a few nodes.

The Ecuadorian SRI dataset had some issues with the details of the data. We found that the Ecuadorian SRI dataset was not entirely accurate. So, we made some changes to the tax-filing frequency metrics. We made sure they were the same. Then we checked the activity codes for each period.

We did this so that we could be certain. We did not want to get false positives. We wanted to make sure the Ecuadorian SRI dataset hubs we found were ghost companies. We did not want them to be people or companies that just file a lot of taxes.

We used the SRI dataset to find these ghost companies in the Ecuadorian SRI dataset.

4.1. Strategic Disarticulation Table

So, we want to make the surgical audit strategy work, we found the ten places that connect everything together; these ten places are like the roads that hold the whole network together. To stop the nodes, we should focus on shutting down these ten main places first. This will help us break down the part of the fake system. The ten main places are listed in Table 1. We need to make sure we deal with these ten places if we want to control the system.

These hubs are basically the masterminds behind the company plan. They have betweenness scores, which means they are in control of how shady information and transactions move across different corporate tax areas. Unlike checking everything at once, which is expensive and not very effective, focusing on just these ten key nodes would instantly disrupt about 45% of the total flow in the network.

This evidence is the same as what Garay-Salamanca and other people found [11]. They say that it is easy for the government to be controlled by these companies because they work together. If we look at these companies, the people who check on the government can start to be more careful and stop bad things from happening. They can make sure that public money is safe and do things the way other

Table 1

Top 10 Critical Nodes for Surgical Intervention.

Rank	Anonymized Node ID (SHA-256)	Betweenness Centrality (C_B)	Degree	Classification
1	8f3a9e...2a1b	0.842	58	Core Hub
2	a1b2c3...d4e5	0.791	42	Strategic Bridge
3	9e8d7c...6b5a	0.715	39	Strategic Bridge
4	1f2e3d...4c5b	0.688	35	Core Hub
5	c4b3a2...f1e0	0.612	31	Hub
6	e5d4c3...b2a1	0.589	29	Hub
7	d3c2b1...a0f9	0.543	27	Hub
8	b7a6d5...c4e3	0.512	24	Hub
9	f9e8d7...c6b5	0.498	22	Hub
10	a2b3c4...d5e6	0.475	20	Hub

countries do to stop corruption. State capture is a problem, and these corporate networks are a part of it. By looking at these companies, we can stop state capture and make sure that public resources are used the right way. State capture happens when these corporate networks are able to control the government [41, 42].

5. Technical Recommendations for SAIs

To help Supreme Audit Institutions use this framework successfully, we suggest the following technical guidelines for changing from traditional auditing to Topological Intelligence. We are talking about Supreme Audit Institutions. How they can use Topological Intelligence.

The goal is to make sure Supreme Audit Institutions can use this framework and move to Topological Intelligence. We want to make this change as smooth as possible for Supreme Audit Institutions.

So we have some guidelines for Supreme Audit Institutions to change from traditional auditing to Topological Intelligence. These guidelines are important for Supreme Audit Institutions and Topological Intelligence:

1. **Dynamic Network Mapping and Cell-Regeneration Tracking:** Audit institutions should stop doing reports once a year. They should update graphs every quarter instead. This is because companies that do things can change quickly. So it is really important to keep track of what's happening all the time. We need to take pictures of what's going on at regular times. This helps us track how fake companies can come back to life after we have looked at them. It also helps us see when companies are going to make changes before they actually happen. Audit institutions need to do this to keep up with corporate networks. These networks are like living things. They can change and grow. We need to watch them all the time to see what they are doing. This will help us catch the companies and stop them from doing bad things. Audit institutions should use quarterly graph updates to do this [15, 37].
2. **Transition Toward Relational Audit Clusters:** Control organizations should stop using divisions that are organized by zone or geographic boundary. They should move toward using audit clusters instead. This means grouping entities according to how closely they are connected, who their shared shareholders are, who their legal representatives are, or where their physical addresses are. This allows auditors to find patterns of zonal collusion that they cannot see when everything is separated into different zones. Control bodies and auditors can use audit clusters to do this. The control bodies will be able to see things that remain invisible when they use the way of organizing things [34, 10].

3. **Forensic Capacity Building and Tooling:** People who work with audits should really know how to use Python to look at networks and understand the RODES model for AI-assisted interrogation. This is an important skill for them to have. SAIs need to keep learning and improving their skills. They should have training programs that combine what they already know about law with computer science. This will help the people who work with audits to work with sets of data. The RODES model and Python are tools for them to know how to use [27, 28].
4. **Standardization of Data Sovereignty Protocols:** To make it easier for different organizations to work together, we think it is a good idea to make sure that everyone uses the same way of securing data when they share it. This means that the SRI, Superintendencia de Compañías, and CGE should all have to use a kind of secure code like SHA-256 when they exchange data. This way they can work together. Share information without breaking any rules about keeping data private. It also means that if there is a problem, the information can still be used as evidence in court [15, 24].

6. Conclusion

This study shows that forensic auditing can really make a difference when it is guided by data. It changes the way audits are done from checking things to actually taking action to make things better. The system we talk about here can be used by government agencies or other groups that oversee things. It is a tool that can be used by people to understand complex networks.

By focusing on the important parts of the network instead of looking at everything, we can really stop fraud from happening. This means that government agencies can take apart the parts of fraudulent networks and prevent them from coming back.

This combination of intuition and computer analysis is the future of making sure the governments are working properly. It helps governments keep up with the ways that people try to corrupt the system and makes sure that the money is safe in the digital age [9, 36, 25].

Declaration on Generative AI

During the preparation of this work, the authors used Gemini AI and Grammarly for grammar and spelling checks, paraphrasing, and rewording. After using these tools, the authors reviewed and edited the content as needed and take full responsibility for the publication's content.

References

- [1] J. C. Aguirre Quezada, M. C. Flores, The corruption in south america. an approach from the forensic audit, 2019.
- [2] C. M. E. Portilla, J. A. R. Zambrano, L. M. C. Quiñonez, M. C. B. Flores, Auditoría forense y su impacto en las organizaciones públicas del ecuador, *Revista de ciencias sociales* 30 (2024) 410–421.
- [3] W. J. C. Velásquez, R. J. C. Rivera, J. A. R. Sanchez, Evasión tributaria: Tendencias, retos y oportunidades. una revisión sistemática, *International Journal of Professional Business Review: Int. J. Prof. Bus. Rev.* 9 (2024) 2.
- [4] L. Castillo-Villanueva, D. Velázquez-Torres, Sistemas complejos adaptativos, sistemas socioecológicos y resiliencia, *Quivera Revista de Estudios Territoriales* 17 (2015) 11–32.
- [5] A. Fonseca, Auditoría forense: Sus fundamentos jurídicos y la praxiología 2a Edición, Ediciones de la U, 2022.
- [6] A. Alexopoulos, P. Dellaportas, S. Gyoshev, C. Kotsogiannis, S. C. Olhede, T. Pavkov, A network approach to detect value added tax fraud, *Journal of the Royal Statistical Society Series A: Statistics in Society* (2025) qnaf205.
- [7] A.-L. Barabási, *Ciencia de redes* (Signa_Lab), ITESO, 2022.

- [8] C. Chen, M. I. Neshkova, The effect of fiscal transparency on corruption: A panel cross-country analysis, *Public Administration* 98 (2020) 226–243.
- [9] V. Giannopoulos, M. Vlachakou, S. Kariofyllas, I. Makris, Corporate governance and tax avoidance: Evidence from greek service-sector firms, *Journal of Risk and Financial Management* 18 (2025) 538.
- [10] G. C. Montes, P. H. Luna, Fiscal transparency, legal system and perception of the control on corruption: empirical evidence from panel data: Gc montes, ph luna, *Empirical economics* 60 (2021) 2005–2037.
- [11] L. Garay-Salamanca, I. De-León, E. Salcedo-Albarán, *Captura y reconfiguración cooptada del estado en guatemala, méxico y colombia*, Bogotá DC: Bogotá: Grupo Método (2010).
- [12] I. Luna-Pla, J. R. Nicolás-Carlock, Corruption and complexity: a scientific framework for the analysis of corruption networks, *Applied Network Science* 5 (2020) 13.
- [13] P. B. Saptano, G. Mahmud, F. Salleh, I. Pratiwi, D. Purwanto, I. Khozen, Tax complexity and firm tax evasion: A cross-country investigation, *Economies* 12 (2024) 97.
- [14] J. J. Rodríguez de la Fuente, G. Assusa, Inequality cannot be evaded. a sociological exploration of tax noncompliance and social stratification in latin america, *Revista mexicana de sociología* 88 (2026) 449–490.
- [15] N. A. Galadanci, G. Hellemann, S. Washko, C. S. Abrams, K. Torres, J. Kanter, Novel use of a hash-based tokenization for sharing sickle cell disease data without sharing protected health information, *Blood Advances* 10 (2026) 3255–3263.
- [16] E. Esenogho, I. D. Mienye, T. G. Swart, K. Aruleba, G. Obaido, A neural network ensemble with feature engineering for improved credit card fraud detection, *IEEE access* 10 (2022) 16400–16407.
- [17] J. Ferwerda, I. Deleanu, B. Unger, Corruption in public procurement: finding the right indicators, *European journal on criminal policy and research* 23 (2017) 245–267.
- [18] C. Redroban-Ortiz, J. Matute-Petroche, L. Rivas-Tovar, X. Torres-Maldonado, *Redes aplicadas a procesos de formación en entidades fiscalizadoras superiores*, 2024.
- [19] A.-L. Barabási, R. Albert, Emergence of scaling in random networks, *science* 286 (1999) 509–512.
- [20] J. R. Nicolás-Carlock, I. Luna-Pla, Conspiracy of corporate networks in corruption scandals, *Frontiers in Physics* 9 (2021) 667471.
- [21] V. D. Blondel, J.-L. Guillaume, R. Lambiotte, E. Lefebvre, Fast unfolding of communities in large networks, *Journal of statistical mechanics: theory and experiment* 2008 (2008) P10008.
- [22] M. E. Newman, Modularity and community structure in networks, *Proceedings of the national academy of sciences* 103 (2006) 8577–8582.
- [23] J. A. G. Caraveo, C. C. De la Rosa Flores, R. M. C. Erives, C. L. R. Rascón, Auditoría 4.0: Viabilidad, desafíos y futuro del uso de ia en despachos contables y financieros, *Estudios y Perspectivas Revista Científica y Académica* 5 (2025) 5844–5862.
- [24] A. K. Hoxha, M. Miti, Transparency, information, sustainability interaction with citizens, vs the fight against corruption, and their role in the public sector auditing. evidence from albania, *Theoretical and Practical Research in Economic Fields* 16 (2025) 425–435.
- [25] R. Mousa, Audit cyber-resilience as a governance capability: Evidence from us gao performance audits, *EDPACS* (2026) 1–9.
- [26] S. Cindori, Beneficial ownership-demand for transparency, threat to privacy, *Rev. Eur. & Comp. L.* 55 (2023) 113.
- [27] T. M. Matras, Harmonisation of the beneficial ownership registers in european union, *Journal of Money Laundering Control* 28 (2025) 81–94.
- [28] C. L. R. Ortiz, L. A. R. Tovar, X. M. T. Maldonado, C. A. A. Alvarado, L. V. J. Sangurima, Redes complejas como metodología para el control gubernamental en procesos de contratación pública en ecuador, *Revista española de la transparencia* (2024) 215–249.
- [29] G. R. Abdi, A. H. R. Sheikhan, S. Kordrostami, B. Zarei, M. F. Rad, Identifying communities in complex networks using learning-based genetic algorithm, *Ain Shams Engineering Journal* 15 (2024) 103031.
- [30] M. Kivel, A. Arenas, M. Barthelemy, J. P. Gleeson, Y. Moreno, M. A. Porter, Multilayer networks,

- Journal of complex networks 2 (2014) 203–271.
- [31] F. Calderoni, D. Brunetto, C. Piccardi, Communities in criminal networks: A case study, *Social Networks* 48 (2017) 116–125.
 - [32] J.-M. Llanos-Mosquera, G.-L. Muriel-López, J.-D. Triana-Madrid, V.-A. Bucheli-Guerrero, Evolutionary algorithms guided by scale-free complex networks, *Revista científica* (2022) 228–241.
 - [33] M. Buchahin, Auditoría forense delitos contra la administración pública, 2015.
 - [34] M. S. Lyra, F. L. Pinheiro, F. Bacao, Public procurement fraud detection: a review using network analysis, in: *International Conference on Complex Networks and Their Applications*, Springer, 2021, pp. 116–129.
 - [35] B. Cuadrado-Ballesteros, A.-M. Ríos, M.-D. Guillamón, Transparency in public administrations: a structured literature review, *Journal of Public Budgeting, Accounting & Financial Management* 35 (2023) 537–567.
 - [36] P. M. Gilmour, Lifting the veil on beneficial ownership: Challenges of implementing the uk’s registers of beneficial owners, *Journal of Money Laundering Control* 23 (2020) 717–734.
 - [37] I. G. García, A. Mateos, Use of social network analysis for tax control in Spain, *Hacienda Publica Espanola* (2021) 159–197.
 - [38] D. Jancsics, Family corruption: Relatives in corrupt transactions, *Sociology Compass* 19 (2025) e70134.
 - [39] M. García-Pérez, J. Silva, Algorithmic opacity and institutional capture: A sociological perspective on corporate tax evasion, *International and Multidisciplinary Journal of Social Sciences* 12 (2023) 112–135.
 - [40] L. C. Freeman, Centrality in social networks conceptual clarification, *Social networks* 1 (1978) 215–239.
 - [41] G. Agostinis, S. Palestini, Transnational governance in motion: Regional development banks, power politics, and the rise and fall of South America’s infrastructure integration, *Governance* 34 (2021) 765–784.
 - [42] M. P. Angueta-López, H. A. Quimbata-Tarco, E. V. ArcosNaranjo, Evolución de las empresas fantasmas e inexistentes y el perjuicio causado al estado ecuatoriano del 2017 al 2023, *Revista Científica Zambos* 4 (2025) 45–60.