EDGELANDS

CITY GOVERNMENTS & OSS VULNERABILITIES: STRENGTHENING CITIES' CYBERSECURITY THROUGH OSS SOLUTIONS

By: Santiago Uribe and Andres Puerto

The Edgelands Institute[1]

We are grateful to Katharina Meyer for her support and encouragement and everyone involved with the DIIF Initiative for their generous grant.

INTRODUCTION

This project focuses on cybersecurity and maintenance vulnerabilities faced by cities and municipal governments. We have chosen to take Colombian cities as a case study to highlight the role of cities and municipal governments in maintaining and supporting Open Source Software (OSS) in this country. It does so from the perspective of the incentives and barriers to adopt and maintain OSS, and the related challenges to cybersecurity. We chose this country based on past Edgelands work with Colombian cities and because - to the best of our knowledge - no comprehensive study has been done in this country regarding its cities' cybersecurity vulnerabilities. We believe the findings and methodology could be applied to other middle-income / developing countries to better craft OSS policies and enhance cybersecurity readiness.

We focus on cities for two main reasons: first, cities are at the forefront of crafting and implementing digitization and smart city policies that require safe, resilient and cost-efficient digital infrastructure. At the same time, cities generate and hold a very large amount of highly valuable data that makes them desirable targets for cyberattacks. Second, Cities are the places where the majority of people live. In general (governance regimes change from country to country, in some contexts it is the national government responsible for this), cities are responsible for providing essential services as well as for building and maintaining critical physical and digital infrastructure. The security of municipal digital infrastructure and software procurement lies at the center of these governance challenges for cities.

Using Colombia as a case study (a middle-income, developing country, not particularly known for its sound OSS ecosystem), we analyze the role that municipal governments and other government entities play in adopting and maintaining OSS and its implications on local cybersecurity. With this project we focus on what Kingsbury et al. *calls the organizational dimension of OSS, defined as (not only) formal OSS institutions, but also cross-cutting regulations, financing, and governance) of OSS).*

We do so in order to develop an analytical framework that best describes the incentives and barriers faced by cities and public entities in adopting and maintaining OSS and the implications this has on cybersecurity. This in turn contributes to focalize future research and policy interventions in similar middle-income, developing cities.

The data we collected through interviews, policy document reviews and right to information petitions helped us understand the state of OSS in Colombian cities and public entities. Building an overview of the OSS and the extent of their use among municipalities allows us to identify the cybersecurity threats that cities are most vulnerable to. With this information city officials are better able to to plan and respond to threats and attacks. This access to timely information that is independently available allows for tailored solutions thus increased readiness and more robust systems.

We then go on to develop a cybersecurity/ OSS vulnerability index through a digital tool where city officials are able to measure threats to their infrastructure based on the OSS programs being used.

[1]Founded in 2021, the Edgelands Institute is a multidisciplinary pop-up organization dedicated to exploring how the urban social contract around the digitization of security is being redefined in cities around the world.The pop-up nature of Edgelands is characterized by two key aspects. First, it reflects the institute's limited lifespan. From the very beginning, Edgelands was designed to be a temporary organization that would exist for only four to five years. This pop-up concept - and the dynamic energy it brings - is central to our work. We believe that a pop-up approach helps break down barriers to accessibility and diversify the experiences of those involved, addressing challenges often found in traditional academic and policymaking circles. The temporary nature of pop-ups generates excitement and raises awareness of the complex issues we address in a relatively short period of time, while bringing together a wide range of stakeholders through active participation. Second, it refers to the way we work on cities and engage with diverse communities and stakeholders to reflect on issues at the intersection of security, digital technologies and the urban social contract. Our "pop-up methodology" involves entering a city for a short period of time, typically about a year, during which we host temporary, interactive events and installations. These initiatives are designed to spark conversations, disseminate information, and encourage collaboration around key themes. After this period, we leave the city - but with the possibility of returning later to revisit the discussions and reflect on the outcomes that emerged from our initial engagement. As a pop-up, we do not aim for a long-term process, but rather to engage the public around issues that are often the province of experts. Our approach is adaptable to the cultural and urban context of each city, an important lesson we have learned. We have continuously tested, adjusted and redesigned our spaces with the aim of creating an open dialogue.

BACKGROUND (LITERATURE REVIEW)

Digital Infrastructure (like physical infrastructure) is critical and requires investments for maintenance. OSS is understood as a system where the copyright holder grants users the right to use, study, change and distribute the software and its source code to anyone for any purpose (UNDP, 2023). The World Bank defines OSS *as software that is readily available with its source code and license, free of cost to anyone who wants to study, change, modify, or distribute it. Historically, it has usually been developed through collaboration or a group or informal network of programmers, who provide the entire source code to the end user* (World Bank, 2019 p. 9). Some commonly used terms for OSS include:

a. Free and Open Source Software (FOSS) – FOSS refers to software that is freely available for users to copy, exchange, share, and use.

b. Free/Libre Open Source Software (FLOSS) – Similar to FOSS, FLOSS provides even greater freedom to edit, modify, and distribute the software in its original or modified form without restrictions. FLOSS highlights the importance of freedom, encouraging users to modify and redistribute the source code with few or no limitations.

In contrast, proprietary software, also known as closed-source or commercial software, is privately developed and typically requires the purchase of a license, either as a one-time fee or through recurring payments. The source code of proprietary software is usually hidden from users. The use, distribution, and modification of this software are restricted by the copyright holder—often the publisher, vendor, or developer. Proprietary software remains the property of its owner/creator and is used by end users under predefined conditions specified in a license. While the source code of open-source software is freely accessible, proprietary software is not.

Whatever its nature, software is essential for developing and maintaining the digital infrastructureI used by municipal governments, which includes the necessary operative infrastructure, services offered to citizens and not least important collecting, managing and storing data.

OSS has many advantages and disadvantages. Amongst others, its complex nature as a “common good”. There are incentives and benefits for its use and “consumption”, but not for its use and investment in maintenance. It is a good that is widely susceptible to vulnerabilities. According to (Sharma 2023) this relies on something called "tragedy of the commons" or more precisely “tragedy of digital commons". This kind of tragedy is related to an excess use of a freely available resource with no commitment to their evolution or security from the technical aspect, being in a role of irresponsible consumer or free rider.

(Wachs et al. 2022) overview of the essential role of software in today's highly services-oriented economy, communications, etc, is widely recognized. Not only is software necessary to keep firms, computers, cars running, the development and licensing of software is in itself a major economic, globalized sector, facilitated by the seamless sharing and distribution of its end products through the web. Hoffman (2024) in turn discusses how if software is an ubiquitous building block of digital infrastructure, OSS is even more so. OSS - defined as software whose source code is publicly available for inspection, use, and modification and created in a decentralized manner and distributed for free (Hoffman et al. 2024) is present in as much as 96% of codebases (Synopsys 2024). Moreover, OSS forms the backbone of nearly all aspects of technology: nearly 97% of applications rely on open-source code, with 90% of businesses integrating it into their operations.

Deploying and maintaining open-source in government requires new skill sets and sustainable business plans for the maintenance of systems. It also requires engagement with open-source communities and local ecosystems due to the decentralized and voluntary nature of OSS projects and contributions. Governments have historically been hesitant to adopt OSS (Cassell, 2008) due to capacity/human resource constraints, knowledge gaps, uncertainties regarding costs, and the absence of robust local and global ecosystems, support structures, and communities for ensuring long-term support, security, maintenance, and sustainability.

(Hoffman et al.,2024) proposes that calculating the value of OSS is inherently difficult to assess given the "non-pecuniary" (free) nature of OSS and the lack of centralized tracking for its uses. In their research, they estimate "supply-side value of widely-used OSS is $4.15 billion, but that the demand-side value is much larger at $8.8 trillion and that firms would need to spend 3.5 times more on software than they currently do if OSS did not exist" (Hoffman et al., 2024).

Similarly, another indicator which illustrates the cost side of software for organizations is the percentage of municipal expenditure on software and maintaining digital infrastructure: a 2015 report on the use of technology by British municipalities (Copeland, 2015) estimates that 6% of their budget is spent on procuring and maintaining digital infrastructure and proprietary software. The report goes on to recommend local governments to *"Phasing out costly bespoke IT systems. Rather than each LA independently designing or commissioning its own apps and online services (such as paying for council tax or reporting noisy neighbours), an 'app store' should be created where individuals, businesses or other organisations can bid to provide them. The services created could then be used by dozens – or even hundreds – of local administrations, creating economies of scale that bring down prices for all"* (Copeland,2015).

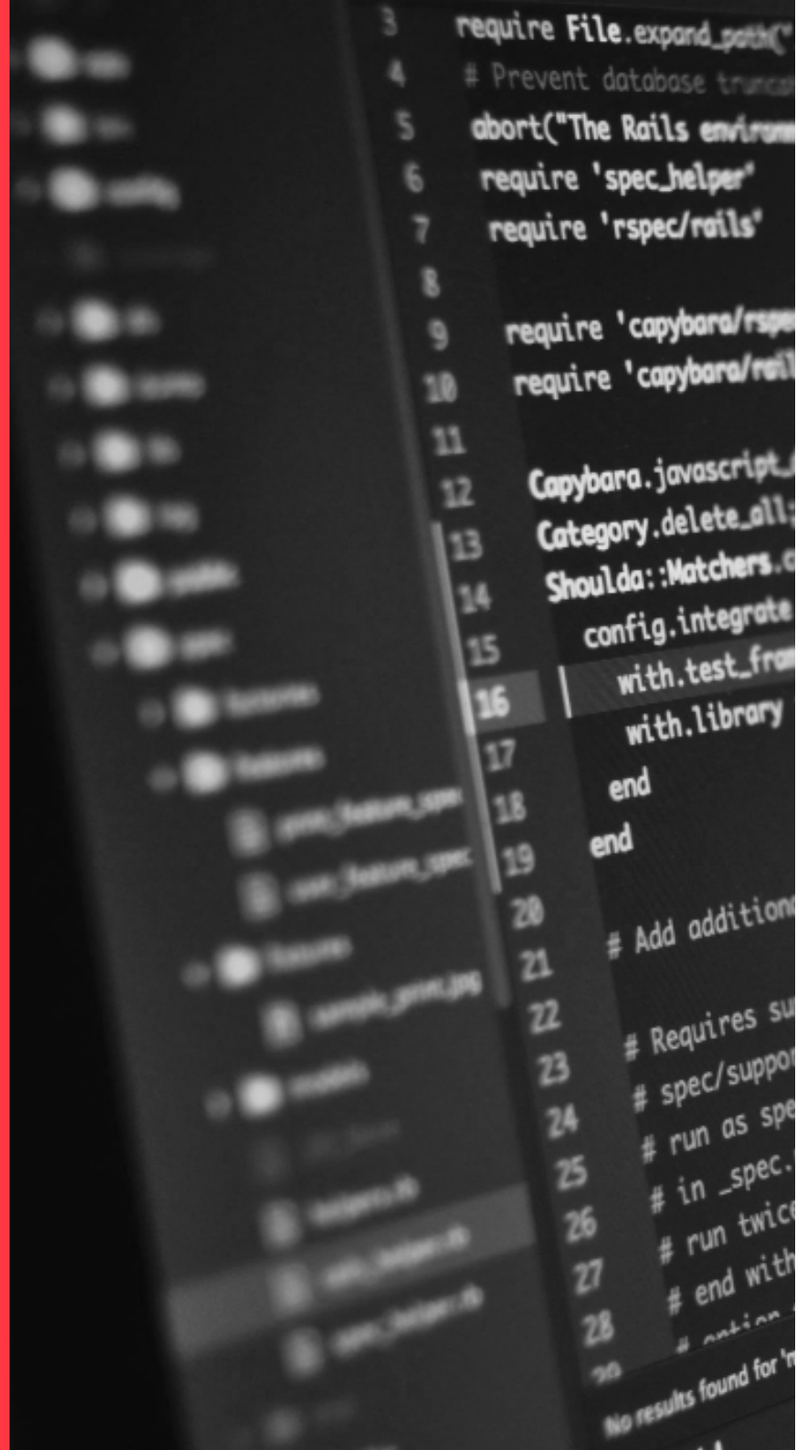
Given the high costs of proprietary software on one side, the value-generating potential of OSS and its advantages on cybersecurity begs the question: why is OSS not more widely used, especially in resource-strapped municipalities? On this, the literature on the barriers, disincentives and drivers of OSS adoption in cities has pointed that governments see OSS solutions as a form and driver of innovation. Thus, if OSS is to be widely adopted or seen as a reliable alternative to the cybersecurity risks faced by municipal governments, support for OSS solutions should be, at least in part, a top-down initiative from city officials in decision-making positions.

In his paper, Cassell highlights that the understanding of Free and Open Source Software (FOSS) in the public sector is limited, with most research focusing on legal aspects such as licensing and its perceived benefits. Less has been researched on aspects of adoption and implementation. His research finds that the main reason why FOSS is attractive for the public sector is due to its cost savings; but reliability, customizability, security, and freedom from proprietary lock-in were also important incentives for adopting FOSS. Moreover, Cassell (2008) argued that the main reason why cities innovate through e-government strategies is to maintain autonomy of their Digital Infrastructure from vendor lock-ins. Secondary incentives included increasing the efficiency and effectiveness of government.

In his study of cities adopting FOSS he found they were motivated by a desire for independence from monopolistic private actors (tech companies), echoing historical efforts by cities to maintain control over essential services (such as utilities, transport). This aligns with literature on state capacity: when threatened by internal or external actors, states protect themselves by increasing their capacity to act. He finds that the primary factor driving innovation was a desire to maintain the capacity in order to resist potential future threats, suggesting future research into public sector innovation and FOSS.

These findings still hold true in the present: The European Commission's "OSS Strategy 2020-2023" cites digital autonomy as the main argument to pursue OSS solutions: *"Open source impacts the digital autonomy of Europe. Against the hyper-scalers in the cloud, it is likely that open source can give Europe a chance to create and maintain its own, independent digital approach and stay in control of its processes, its information and its technology"* (European Commission, 2020 #5).

Open-source solutions are poised to gain significant traction among policymakers in developing countries, where software markets are less developed and concerns about vendor dependence are prominent. In such contexts, there is a heightened need for public sector preparedness and investments in DI.



THE ROLE OF SOFTWARE IN MUNICIPAL GOVERNMENT

Software and DI are the building blocks of the many services a city should offer its residents: traffic solutions, utilities, housing, health services. These softwares plan an essential role in building applications, developing digital products and analyzing data, among other elements of smart cities and digitization strategies. Digital infrastructure is conceived of as the hardware, software, and organizational and institutional settings for transferring (e.g., networks/transmission), storing (e.g., cloud data storages), accessing (retrieving as machine-readable), processing and/or using digital data (done by using algorithms and depending on computational power; Henfridsson & Bygstad, 2013; Scholz et al., 2018). Yet, the technical and organizational layer "allows multiple stakeholders to orchestrate their service and content needs" (Constantinides, Henfridsson, & Parker, 2018, p. 381). Thus, the "good is not the infrastructure system itself, but the functionalities that it affords" (Constantinides & Barrett, 2015, p. 42). At the same time, municipal governments require software solutions and services for their functioning and operation. Therefore, investments in development and maintenance of software and DI are necessary for city government operations and as important as other kinds of infrastructure. Cities are then faced with choosing between proprietary software or OSS. Understanding the barriers and incentives for choosing either can begin to shed light on the structural barriers that limit widespread adoption of OSS, the role of cities in the wider OSS ecosystem and the issue of cybersecurity (Sharma, Matczun).

The literature on public sector adoption of OSS suggests different drivers and motives that make a public institution to implement OSS systems. Lostri and Wood, (2023), from the Center for Strategic and International Studies of over 600 policy instruments related to OSS promotion in countries around the world found that the "main reason (43% of the reviewed sample) why governments sought to promote OSS was modernization(...) including efforts at digitization, e-government, interoperability, and training to increase awareness and capacity.

Moreover, the survey identified "the use of OSS by the government as a way to help increase transparency on how funds are used by the government and how procurement is secured. Especially in South America, the links between OSS and sovereignty are strong. Governments perceive OSS as a way to achieve technology sovereignty and autonomy- they seek to avoid dependency on foreign technology" (Lostri & Lewis, 2023).

The advantages of using OSS have not gone unnoticed in the public sector. Perhaps one of the most well-known users of OSS in the public sector is the municipality of Munich. It started a plan to migrate to OSS in 2003 with the aim to finish the migration of all of its 12.000 workstations by the end of 2012. The cost of its migration project is € 11,7 million, while an upgrade to a comparable environment based on Microsoft Windows and Office would have required € 15,52 million, excluding costs of € 2,8 million for license fees for upgrades recurring every 3 to 4 years for a Microsoft infrastructure. The French national police force decided to migrate to OSS in 2004. This enabled the organization, which had 90.000 workstations in 2004, to save over €50 million on software licenses, hardware and maintenance since the migration was started.

Yet, beyond financial cost considerations, governments are driven to pursue other objectives when implementing OSS systems. (Lostri and Wood, 2023) review of OSS policies found that modernisation and support for industry were top stated objectives in said policies. In that same study, cybersecurity and sovereignty (independence from vendor lock-in) were also widely mentioned as objectives in OSS policies. The literature then points out that municipalities have the incentives and knowledge of the trade-offs involved in using OSS. One aspect that requires better understanding is the organizational aspect of OSS. Here we believe municipal governments hold more sway: through DI policy and cybersecurity protocols, procurement processes and support for OSS projects, they could harness the benefits of OSS in improving cybersecurity.

Developing and sustaining open source software (OSS) depends on a combination of technical aspects (such as the engineering and maintenance of open source code), social elements (including the communities that form around specific OSS projects), and organizational dimension (such as formal OSS institutions, along with overarching regulations, funding, and governance). As a result, legal and governance frameworks play a crucial role in shaping the development and maintenance of the digital infrastructure of open source software.

Whilst a large part of the literature deals with the technical and social dimensions of OSS, we find that less has been explored about the organizational dimension of OSS. Except for the considerable literature on cyber security issues related to digital infrastructure in cities, the focus has not been on exploring and proposing institutional arrangements whereby cities can develop, support and adopt OSS solutions, by for example financing developers communities.

A standout example is the City of Amsterdam, which is both a user and contributor to OSS, and in many ways a model for how a city should approach OSS. This case underscores the potential for cities to not only adopt but actively contribute to OSS initiatives. The city started a plan to migrate to OSS in 2003, with the aim to conclude the migration of all 12.000 workstations by the end of 2012. Open source software (OSS) adoption has gained significant traction in the Netherlands over the past two decades.

A comprehensive policy landscape has emerged, complemented by concrete implementation efforts across national and local government bodies.

At the national level, the Ministry of Interior and Kingdom Relations (BZK) has emerged as a key driver, establishing an Open Source Program Office (OSPO) to steer the government's open source agenda. Major policies like the Open Government Act and a proposed revision to the Competition Act mandate transparency and facilitate OSS adoption. The government has also conducted extensive studies exploring the costs, benefits and legal aspects of releasing OSS. (Thévenet et al.,2023) Overarching strategies like the Digital Government Agenda (2018) and NL DIGITAAL (2019) have provided strategic impetus for OSS use across public administration. Implementation is further supported by the public software procurement playbook and the establishment of the Standardisation Forum which mandates open standards.

Numerous public entities have embarked on pioneering OSS initiatives. Amsterdam has developed a comprehensive open source policy complemented by an algorithm register. Educational initiatives like OMOOC (2022) aim to build OSS capabilities. Key agencies like Logius and Kadaster have shared code repositories.

Local governments have been equally proactive, with Amsterdam, Rotterdam, and Groningen transitioning to open source office software and developing digital participation platforms leveraging OSS. Innovative projects harnessing OSS span diverse domains like land mapping, forensics, policing, and open data exchange (Logius, 2019). A vibrant ecosystem of strategic players like the OSPO Knowledge Network, Code for NL, industry associations and foundations actively promote OSS adoption and community building across the Netherlands.

Barcelona's case is another interesting fact of how public entities are adopting OSS infrastructure (Ajuntament de Barcelona,2017). The city established a comprehensive "Open Digitization Policy" through the Government Measure for Open Digitization: Free Software and Agile Service Development in Public Administration in October 2017. This policy is reinforced by guiding documents outlining a code of technological practices, guidelines on technological sovereignty, and public procurement guidelines for information and communication technologies (ICT).

A key aspect of Barcelona's approach is the development of detailed guidelines tailored for the Municipal Computing Institute (IMI) staff to effectively leverage OSS solutions. These guidelines, anchored in the principles of the 2017 policy measure, aim to maximize the benefits of OSS while mitigating potential risks. The primary advantages identified include maintaining technological sovereignty and control over the city's computing systems and citizen data, promoting local software industries, increasing transparency, avoiding vendor lock-in, and enabling cost savings through shared resources and elimination of license fees.

Notably, the guidelines codify established best practices that have emerged from successful OSS projects, spanning technical, legal, and project management aspects. These practices are geared towards enabling diverse participation, maintaining product quality, and may differ from traditional software development methodologies. By adapting these practices as recommendations, the guidelines facilitate IMI's learning process and decision-making framework when working on OSS projects.

The guidelines draw extensively from authoritative resources such as Karl Fogel's paper on "Producing Open Source Software" (2017) and the European Commission's "Guideline on Public Procurement of Open Source Software". This approach aligns Barcelona's efforts with established best practices and legal considerations in OSS adoption within public administration. Overall, the literature highlights Barcelona's holistic strategy towards mainstreaming OSS across the city's digital services and governance. This is achieved through a multi-pronged approach encompassing comprehensive policies, procedural guidelines rooted in community best practices, strategic collaborations with local industry, and capacity building within the public workforce.

CYBERSECURITY CONSIDERATIONS FOR AND IN CITIES

Cybersecurity vulnerabilities are a top priority for municipal tech officers. Since cities produce and store large amounts of valuable data, they are under the constant threat of cyberattacks. In the United States, “nearly half of local governments in a 2016 survey reported being under attack either hourly or daily” (Norris, et. al, 2023). Faced with these constant attacks, city governments must evaluate what types of software are best equipped against these threats and vulnerabilities. OSS offers, in theory, a high level of protection and resilience against cybersecurity concerns. This is what scholars and practitioners deem the thousand eyes principle: the idea that with enough people inspecting open source code, vulnerabilities will be discovered and corrected faster (Sharma 2022). However, in practice, vulnerabilities to cyberattacks are both a deterrent and incentive to opt for OSS solutions. Moreover, this thousand eyes principle can be hard to scale for larger, more complex projects or for large organizations such as municipal governments who often require prompt, constant customer service, solutions and fast reaction to cyberattacks.

The ubiquity of open-source software across nearly every economic sector and its widespread use in critical infrastructure necessitates efforts to enhance its security. Challenges in securing open-source software include its often volunteer-driven and decentralized development model, difficulty identifying all open-source components, and the prevalence of memory-unsafe programming languages.

In 2023, the Biden-Harris Administration made several key initiatives through the Open-Source Software Security Initiative (OS3I) (White House, 2024) to improve open-source software security. First, the OS3I worked to unify the federal government's position and coordinate efforts on this issue across agencies. The Cybersecurity and Infrastructure Security Agency (CISA) released an Open Source Software Security Roadmap outlining a strategic approach for the government's secure use of open-source software and securing the broader ecosystem.

To encourage investment, the National Science Foundation issued a call for proposals on securing open-source software. Additionally, federal agencies engaged the open-source community through a Request for Information to gather input on focus areas like securing open-source foundations, sustaining communities, incentives, research and development, and international collaboration.

The widespread presence and transformative potential of open source software has been widely recognized, leading governments and organizations globally to adopt open source policies and strategies. The European Commission aimed to leverage this innovative and collaborative power through its 2020-2023 Open Source Software Strategy (European commision,2020). The strategy aligned with and supported several overarching EU policies and initiatives. These included the President's call for achieving technological sovereignty in critical areas, the European Interoperability Framework's push for open source usage and contributions, the Commission's digital strategy for transformation, the Digital Europe programme, the EU data strategy and the Tallinn Declaration on leveraging open source in e-government.

Key goals outlined were progress towards digital autonomy by reducing vendor lock-in, implementing the digital strategy through open collaboration, sharing knowledge as a public good, contributing to the open source ecosystem and building world-class digital public services. The governing principles centered around prioritizing open source when feasible, transforming to an open source working culture, sharing code, contributing back to communities, ensuring security and promoting open standards.

EMERGING ISSUES IN OSS AND CITY GOVERNMENT

The literature on open-source software (OSS) adoption in government highlights diverse motivations, challenges, and opportunities, ranging from cost-saving to enhancing transparency, security, and digital sovereignty. Across different contexts, researchers have emphasized both strategic benefits and operational difficulties in adopting OSS within public sector organizations.

From the literature, we can extrapolate at least four emerging issues that inform our assumptions and framework as we dove into our interviews and data collection:

- **STRATEGIC AND ECONOMIC DRIVERS**
  Several studies emphasize the cost-efficiency and strategic flexibility that OSS offers to government bodies. For instance, Shaikh and Cornford (2012) point out that OSS adoption is not just a matter of saving money but also fostering innovation and greater control over software customization to meet specific governmental needs.

  Similarly, Cassell (2020) finds that cities like Munich and Vienna adopted OSS to reduce reliance on proprietary vendors and increase transparency.

- **CHALLENGES IN RISK MANAGEMENT AND IMPLEMENTATION**
  While the benefits of OSS are clear, multiple authors also underline the challenges in risk management and operationalization. OSS adoption often demands new organizational structures and processes, and many public sector entities struggle with this transition. Shaikh (2012) and Lostri highlight the need for stronger policy frameworks and institutional support to overcome technical challenges and security risks.

- **CYBERSECURITY VULNERABILITIES** The issue of cybersecurity is a critical concern, as pointed out by Sharma (2022) and Mateczun. The "tragedy of the digital commons," described by Sharma, explains that OSS suffers from underfunding and insufficient maintenance, leaving governments vulnerable to cyberattacks. Mateczun's research further highlights the underpreparedness of local governments in terms of cybersecurity, despite being frequent targets of attacks. This calls for greater investment in cybersecurity infrastructure and intergovernmental cooperation.

- **GOVERNMENT'S ROLE AND DIGITAL SOVEREIGNTY**
  A recurring theme is the government's role in promoting OSS for broader public sector benefits. Lostri and Wood focus on national policies that support OSS to increase digital sovereignty, encourage interoperability, and strengthen local technology ecosystems they advocate for the creation of open-source program offices (OSPOs) and shared knowledge frameworks to standardize OSS use across government agencies.

The literature underscores a complex and multi-faceted landscape for OSS adoption in the public sector. While the potential for innovation, cost-saving, and enhanced sovereignty is clear, significant challenges remain, particularly in terms of managing cybersecurity risks, organizational change, and ensuring sustained support for open-source initiatives. Governments at all levels must carefully balance these factors to maximize the benefits of OSS while addressing its inherent challenges. Now, our project applies this framework into understanding how organizations and cities with budgetary constraints and cybersecurity vulnerabilities can address some of those analytical categories. In other words, how can a city's institutional and operational capacity be strengthened in order to integrate OSS into their digital infrastructure.

Using Colombian cities as a test case to apply this framework, we aim to understand the status of OSS usage, particularly in city governments. A diagnosis such as this can lead to identifying the barriers to more widespread use of OSS and verify if the cybersecurity is in fact the main deterrent to cities preferring OSS.

METHODS

Our data collection involved conducting a series of semi-structured interviews with IT technicians and city officials responsible for overseeing cybersecurity. In addition, we filed over 12 formal information requests with the Secretariat of IT for major cities across the country. Written questionnaires were distributed as part of these requests, and we received responses from all the cities approached. These official requests, made under the citizens' right to access public information, ensured formal, legally enforceable responses from the relevant authorities.

First, we ran a metadata scraping tool on the infrastructure hosting the websites of 209 public institutions, including municipal governments. The database is publicly available in the Colombian government open data repository. We managed to scrape data from 169 sites related to web hosting and software use. In a second data gathering stage we looked at the Information Technology Strategic Plan (PETI for its spanish acronym) documents. In Colombia every municipality and public entity is required to draft and implement a PETI. These documents contain an overview of the different IT tools, protocols, practices and in general all IT solutions and architectures used by each entity. The objective of the PETIs is to establish a clear roadmap and investment plans for all of the digital infrastructure requirements of each entity (of each city in this case). The majority contain an overview of all the software and hardware required, procurement plans, internal and external host services and plans to develop products or projects within the city's IT ecosystem.

As such, this policy document provided us with valuable input to determine what type and to what extent are colombian cities using OSS in their digital infrastructure.

These policy documents are publicly available and could be easily accessed. We collected over 57 (28 out of 32 for state governments and 29 out 32 for state capital cities) PETIS. Once collected, we run the documents through a document scanner to code for key words, including terms such as OSS, python, oss software, etc (see figures in discussion session). After scanning the documents, and in combination with coding the interviews and written responses we identified a set of emerging issues to build an analytical framework under which to understand the barriers hindering more widespread adoption of OSS.

DISCUSSION AND RESULTS

Colombian tech and software policy is centered on the principle of tech neutrality, whereby "organizations are free to choose the most appropriate technology suited to their needs and requirements for development, acquisition, use, or commercialization, without dependencies on implicit knowledge such as information or data. "*In a written response, a Ministry official explained that tech neutrality "ensures autonomy in the decision making of public entities and municipal governments to adopt and use any kind of software required and to build their digital infrastructure".* Even when the central government sets some guidelines and recommendations, no overarching national legal framework exists and so cities and local governments are left to decide their own software solutions. This situation creates a patchwork of tech policy governance that pose a series of challenges to cities, not least of those cybersecurity issues that leave municipal digital infrastructure underfunded and vulnerable.

At the central, national level, Colombian efforts to foster and implement OSS solutions are relatively new with the Ministry of Information Technologies (MINTICS) officials, Colombia launching a national OSS initiative in 2017. From our interviews and processing of written responses, a series of recurring themes about the barriers to OSS in public digital infrastructure emerged: knowledge gaps, expert human capital, resistance to change, and lack of technical support in cybersecurity issues. Despite these barriers, institutions and IT offices recognize the advantages of open-source software for diverse reasons and as included in their PETI documents. Yet from the data we are able to deduct a different narrative. We manage to map and build a picture of the landscape of OSS usage in Colombian public institutions. In doing so we are able to understand the extent of OSS penetration in Colombia and point to specific policy objectives that address the barriers to OSS finding a stronger foothold in Colombia. We hypothesise that cybersecurity and the private vendor solutions offered by proprietary software are a major hindrance to OSS adoption. In that sense we propose and develop a cybersecurity vulnerability scanner that would allow cities in real time to address cyber vulnerabilities thus strengthening city governments in addressing a general concern when adopting OSS in their digital infrastructures.

LANDSCAPE OF OSS IN COLOMBIA

We sampled 169 cities in Colombia using open databases to determine the number and the type of hosting service (OSS or proprietary). Results revealed that a significant majority, approximately 75%, of these cities' websites are hosted on proprietary license servers. Conversely, approximately 25% of the remaining cities opted for open-source server solutions. Notably, within this subset, nginx emerged as the predominant choice, constituting 16% of the total (Figure 1).

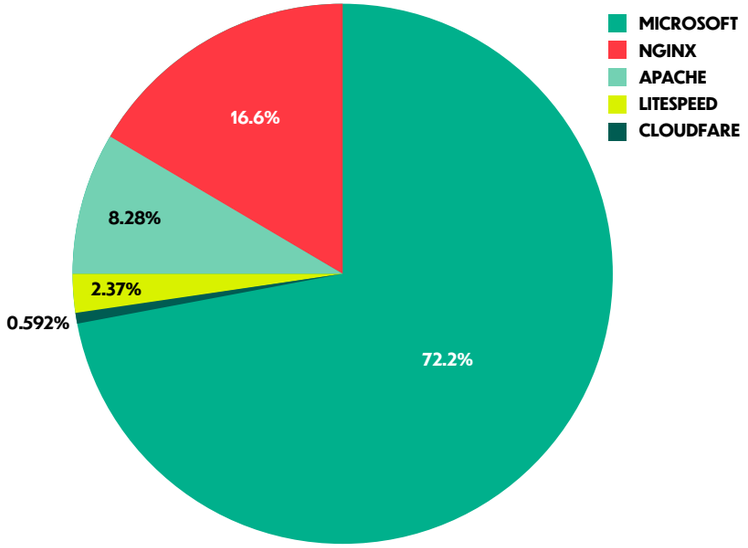


Figure 1

On the other hand, an analysis of the geographic distribution of server licenses among Colombian cities, as depicted in the provided map (Figure 2), reveals an absence of discernible patterns. Notably, certain major urban centers such as Bogotá and Cali, characterized by substantial financial resources, exhibit a preference for open-source server solutions. Conversely, smaller municipalities such as Puerto Carreño or Paipa, operating within comparatively constrained budgetary frameworks, tend to rely on proprietary server licenses.

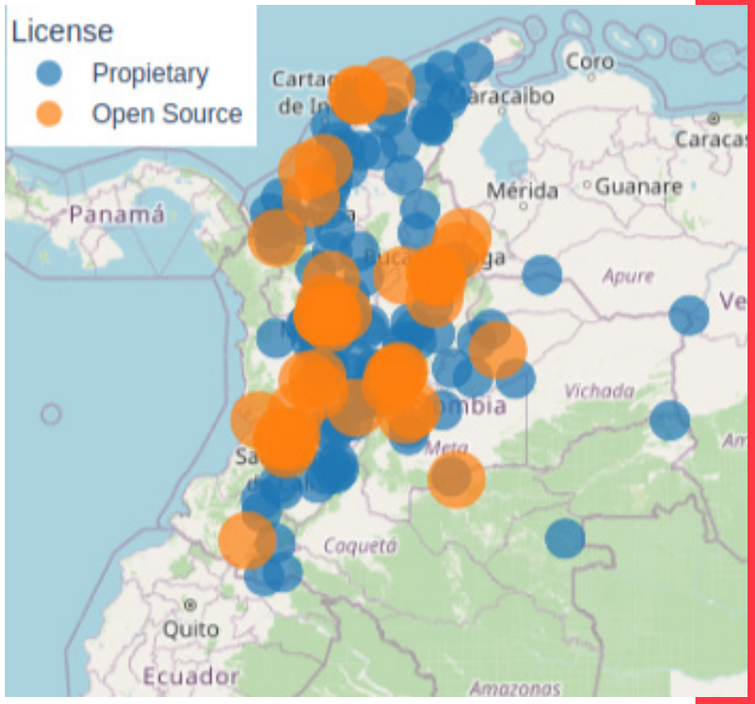


Figure 2. Geographic distribution of servers depending on the license type.

It is important to note that data was successfully obtained from 23 out of the 32 Colombian capital cities, representing a coverage of 72%. Among these capital cities, approximately 48% (11 out of 23) have opted for open-source servers. In contrast, non-capital cities, totaling 146 in our dataset, demonstrate a markedly lower adoption rate, with only 21% utilizing open-source servers (Figure 3).

Our comparative analysis of server licenses across Colombian cities, based on Information Technology Strategic Plans (eg.PETIs in spanish), open data initiatives, and responses to information requests, shows that the choice between open-source and proprietary software is not solely a citywide decision. Instead, it often hinges on decisions made by municipal authorities or by private contractors involved in IT management. This variation suggests that software selection aligns with specific objectives outlined in municipal PETIs or contractors' practices, rather than a standardized approach across cities.

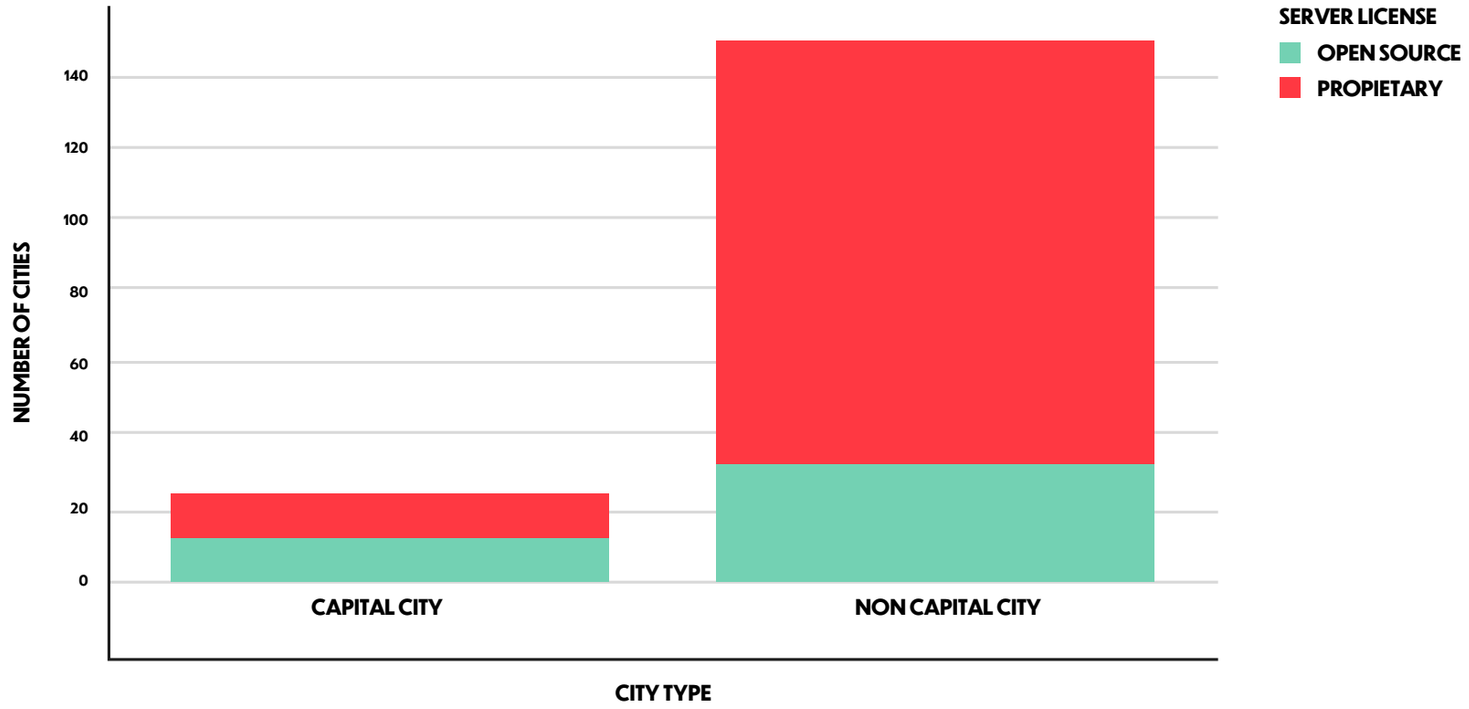


Figure 3. Preferences of license type in function of city Category.

COLOMBIAN STRATEGIC INFORMATION AND TECHNOLOGY PLAN (PETI)

As mentioned, every Colombian public entity is mandated to develop a Strategic Information and Technology Plan. This plan is essential for establishing the primary standards of their technological infrastructure, thereby promoting the adoption of technology and advancing best practices in information technology (IT). Although open source solutions are frequently included in these plans, they are often not explicitly mentioned in the official documents.

The implementation of a Strategic Information and Technology Plan ensures that public entities can systematically address their technological needs and challenges. By setting clear standards and guidelines, these plans help to create a cohesive and interoperable IT environment across various government sectors.

This not only improves operational efficiency but also enhances the quality of public services provided to citizens. Furthermore, a well-structured plan facilitates better resource allocation, ensuring that technological investments are made strategically and yield maximum benefits. The inclusion of open source technologies, albeit often implicitly, plays a significant role in this context, offering scalable and adaptable solutions that can be customized to meet specific needs while fostering community engagement and innovation.

In addition to establishing standards and promoting best practices, these plans play a crucial role in fostering innovation within the public sector. They encourage the exploration and adoption of new technologies, enabling public entities to stay abreast of global advancements in IT. This proactive approach to technology management helps to drive digital transformation, making government operations more transparent, responsive, and effective. By leveraging open source technologies, even when not explicitly documented, Colombian public entities can benefit from a global pool of knowledge and resources, accelerating the pace of technological advancement and ensuring sustainable growth. Ultimately, the strategic integration of information and technology, supported by open source solutions within public entities, support Colombia's broader goals of modernization and economic development.

We conducted an analysis and found that 28 out of 32 state government IT departments and 27 out of 32 capital city IT departments had published a PETI document (Strategic Information and Technology Plans). Our study revealed that at least 47% of the state government PETIs and 56% of the capital city government PETIs included terminology related to OSS (Open Source Software) tools or open source expressions. However, it was observed that these documents do not explicitly acknowledge the significance of open source software for their operations and strategic objectives.

Terms such as *código abierto*, *software libre*, *GNU*, *GPL*, and *open source* are the most frequently occurring OSS-related keywords identified in these plans. The following graphics illustrate the frequency of these terms in each analyzed PETI for both state governments and capital city governments. (Figures 4 and 5)

In terms of software tools, words such as *Linux*, *Ubuntu*, *MySQL*, and *PHP* emerged prominently across numerous cities and state governments. Surprisingly, smaller cities demonstrated a robust adoption of open source tools, rivaling larger urban centers like Bogotá.

Figure 4. Oss related key-words for state governments

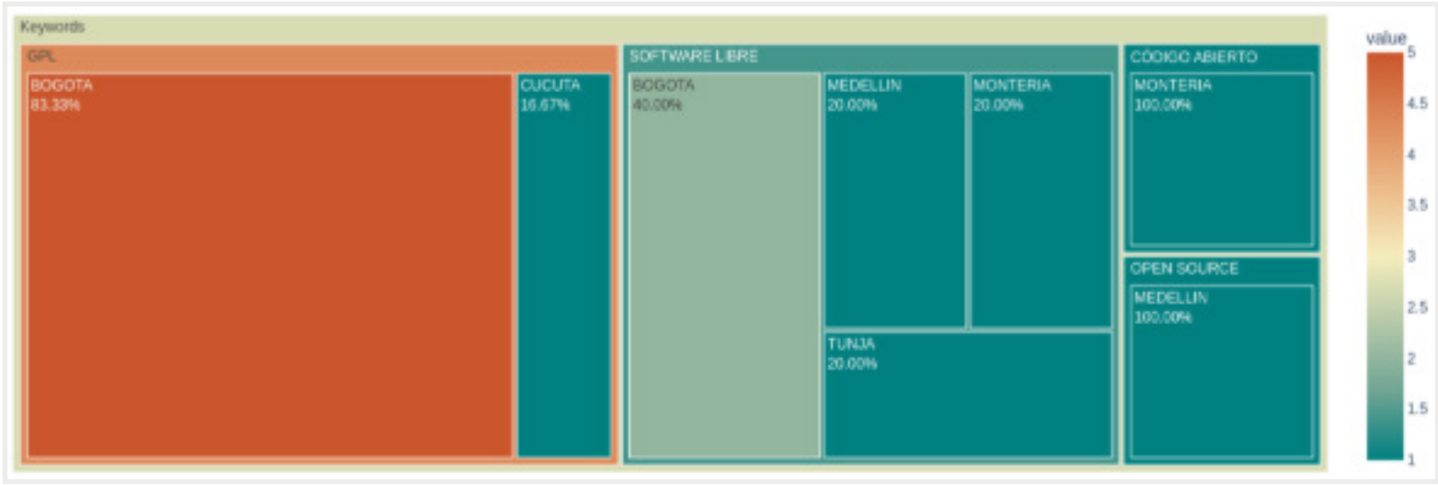


Figure 5. Oss related key-words for capital cities governments

Figure 6. Oss tools mentioned on PETIs state governments

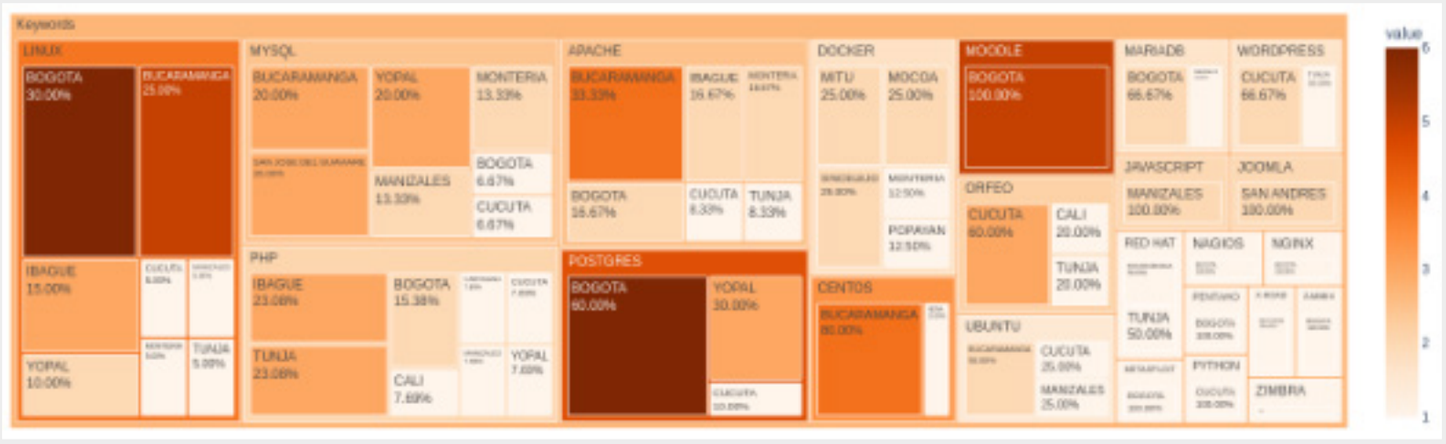


Figure 7. Smaller cities like Bucaramanga demonstrates wide usage of open Source tools

We developed a visualization tool encompassing all these PETIs, accessible at the following link: https://petianalisis.onrender.com/

REQUEST OF INFORMATION PETITIONS

Requests for information petitions were submitted to the local authorities of 11 selected cities. The requests sought detailed responses regarding their adoption of OSS, the extent of its integration into their digital infrastructure, and handling of cybersecurity incidents.

Request for information petition (derecho de petición in Spanish) is a constitutional right allowing citizens to request information, seek clarification, or make formal inquiries to public authorities or private entities that provide public services.

On tables 1 and 2 are the key topics explored within each area.

After compiling responses from formal information petition requests sent to city authorities, a quadrant-based plot (Figure 8) was developed to visually represent the relationship between open-source software (OSS) usage and the occurrence of cybersecurity issues across various cities. Each point in the plot corresponds to a specific city, classified into one of four quadrants based on its characteristics.

OPEN SOURCE USAGE INSIDE PUBLIC AGENCY
OSS strategy exists inside the organization.
Organization is fostering an OSS community in their geographic area?.
Kind of licenses (OSS/proprietary) used inside Digital Infrastructure.
Entities are contributing to an OSS repo?.
IT Ministry OSS initiative awareness.
Awareness of open source software running inside proprietary software.

Table 1. Open source Usage related topics

CYBERSECURITY ISSUES
Digital infrastructure is hosted internally or is hosted through third party vendors.
Public entities experienced cyber attacks?.
Public entities have a cybersecurity protocol.

Table 2. Cyber security issues

➔ TOP RIGHT QUADRANT:

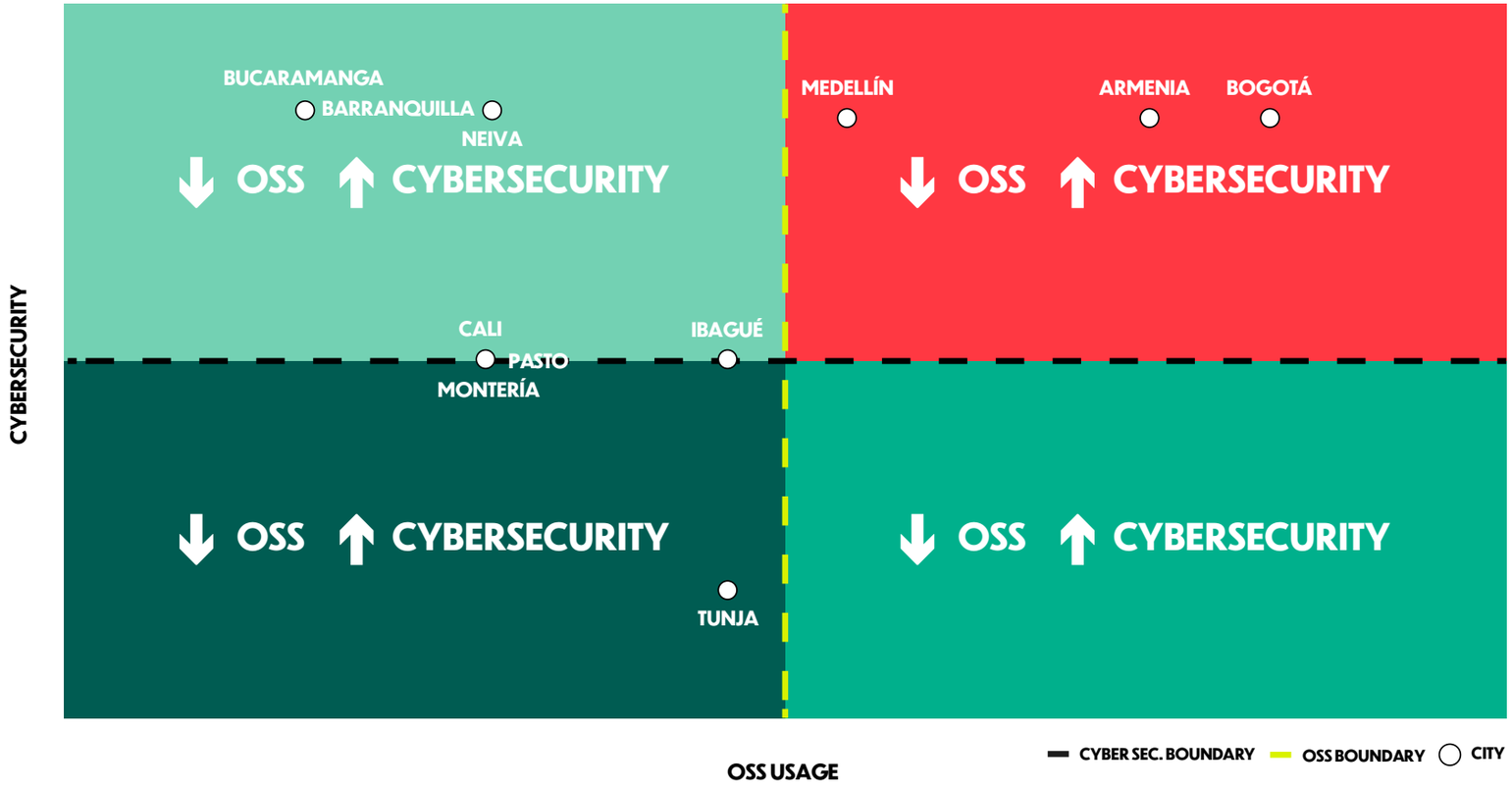
This area represents cities with extensive open-source software usage and no significant cybersecurity issues. These cities are considered to be effectively utilizing OSS while maintaining appropriate cybersecurity measures.

➔ BOTTOM LEFT QUADRANT:

This region reflects cities that may be experiencing cybersecurity issues and demonstrate limited adoption of open-source technologies. In many cases, these cities may also lack well-established security protocols, increasing their susceptibility to cyber threats.

➔ BOTTOM RIGHT QUADRANT:

Cities in this quadrant would typically exhibit high open-source software usage but face ongoing cybersecurity challenges. However, in this study, no cities were found in this quadrant, suggesting that extensive use of open-source technologies has not been clearly associated with cybersecurity issues in the analyzed data.



➔ TOP LEFT QUADRANT:

This region represents cities with good cybersecurity practices but limited use of open-source tools. While they demonstrate strong security protocols, these cities have yet to fully capitalize on the advantages of OSS.

This quadrant plot illustrates that the adoption of open-source software can be a viable option for cities looking to strengthen their cybersecurity, save costs, and reduce their dependency on proprietary software licenses. Open-source tools offer flexibility and cost-effectiveness without compromising security, making them an attractive alternative for public authorities.

It is also important to note that proprietary software, when properly implemented, can mitigate cybersecurity risks. However, the data suggests that open-source usage and cybersecurity issues are not directly correlated, and robust security can be achieved through a variety of software solutions, whether open-source or proprietary.

OSS CHALLENGES AND OPPORTUNITIES FOR COLOMBIAN CITIES: A TEST CASE

Given the Edgelands Institute previous work in the Colombian city of Medellín we delved into understanding this city of over 2.5 million people. The city has a long tradition of entrepreneurship, innovation and tech development. Recently the city underwent an administrative reorganization to become a special technology, innovation and software hub. This allows the city to pool and leverage resources for fostering a tech hub. Asked about why their city did not opt in for more OSS solutions, the Undersecretary of IT in Medellín explained that the city has not yet adopted an official position or strategic plan to increase the use of open-source software (OSS) within its digital infrastructure. This decision is partly to avoid excluding local corporations from providing software services, ensuring that proprietary software vendors can still compete in the city's market. As a result, the municipality currently operates with a mix of both open-source and proprietary software to meet its IT needs.

However, several limitations hinder broader OSS adoption. A key challenge is the lack of human capital, with too few workers skilled in OSS and local salaries that are not competitive enough to attract or retain such talent. Moreover, procurement laws present structural barriers, as they remain tailored to traditional contract markets, where payments are based on deliverables rather than iterative innovation. This rigidity discourages the experimental nature of software development, where testing and adapting are essential but seen as costly under current city budget constraints. Furthermore, drafting Terms of Reference (ToR) for hiring development teams is complex because software projects can evolve during their lifecycle, making it difficult to predefine outcomes clearly. Additionally, the city has faced significant cybersecurity threats, most notably targeting its emergency call center, which underscores the urgency of addressing its digital vulnerabilities.

On the positive side, Medellín's commitment to its smart city policies creates strong incentives for OSS adoption. The city generates and processes vast amounts of data, which could benefit from the flexibility and customization OSS offers. There are discussions about establishing a dedicated fund to support OSS developers, and initiatives like the city's innovation center and Software Valley aim to incorporate education components to train developers specifically in open-source technologies.

Nevertheless, there are significant challenges related to cybersecurity and OSS adoption (Table 3). The city's IT budget lacks a dedicated line item for cybersecurity, and insufficient salaries make it hard to hire qualified security staff. Moreover, top leadership has not prioritized cybersecurity or open-source solutions, leaving a gap in organizational culture and awareness. Staff often lack understanding of both the potential benefits and risks of OSS, which makes it difficult to allocate time and resources to researching and implementing open-source alternatives compared to more familiar proprietary options. Smaller local governments, in particular, face even greater difficulties due to their limited IT resources and expertise, making the proper evaluation, implementation, and maintenance of OSS challenging.

Whilst there is generally a positive view and receptiveness to OSS in city governments, significant barriers in human capital, rules of procurement, cybersecurity, and organizational culture must be addressed for open-source software to become a viable and secure option in the city's digital infrastructure.

After reviewing and analyzing the data collected from the information requests submitted to various cities, we found that the use of open-source software in the context of cybersecurity in Colombian cities faces significant challenges and barriers. One of the main difficulties is resistance to change by public officials, who prefer using proprietary software they are more familiar with. This type of resistance slows the adoption of more open and flexible technologies, delaying the modernization of technological systems. Additionally, compatibility with legacy technological infrastructure is a recurring obstacle, as many public entities rely on outdated systems that make the transition to open-source solutions difficult. Adding to this is the perception of security risks associated with open-source software, generating distrust in its implementation.

BARRIER	DESCRIPTION
Human Capital	Limited skilled workforce in open-source software (OSS) and non-competitive salaries hinder OSS adoption.
Rules of procurement	Procurement laws are outdated, designed for traditional contracts, and not suited to the iterative development process required for OSS projects
Cybersecurity	Lack of dedicated budget, insufficient staffing, and leadership prioritization make the city vulnerable to cyberattacks, impacting OSS implementation
Organizational culture	Limited awareness and support for OSS among staff and leadership, alongside challenges in allocating time and resources for OSS adoption.

Table 3: Perceived barriers to OSS

Moreover, many Colombian cities exhibit a tendency to be free riders in their usage of open-source tools. While they frequently rely on these technologies, there is often a lack of awareness regarding the critical importance of open source in their operations. This underappreciation may lead to missed opportunities for leveraging the full potential of open-source software, particularly in enhancing cybersecurity measures and improving overall efficiency. By not fully recognizing the value of open source, these cities risk stagnation in their technological advancements and cybersecurity readiness, ultimately hindering their ability to effectively address the challenges they face.

Another major barrier is the lack of clarity in the guidelines and policies for adopting open-source software. In some cases, the directives are not specific or fail to provide sufficient guidance

on how to integrate these technologies into existing infrastructures. Moreover, the way digital infrastructure contracts are structured poses a significant challenge, especially regarding support licenses. Many cities rely on proprietary software contracts that include robust support services, while open-source solutions often lack equivalent support due to budget constraints. This limitation makes it difficult for public entities to establish dedicated open-source support teams for each development, further hindering adoption.

There is also a general lack of resources and comprehensive frameworks to promote the widespread use of open-source software in public administrations. Limited technological infrastructure and the absence of collaborative workspaces are additional hurdles that restrict progress toward the large-scale implementation of open-source solutions.

However, there are also significant opportunities in this landscape. The institutional commitment of some administrations to promote open-source software, along with collaborations with the academic sector (eg. FLISOL), provide space for innovation and the development of local solutions that address technological and security needs. Organizing events and providing continuous training to staff are tools that can accelerate the adoption of open-source software, creating a more active and skilled community. Despite the mentioned barriers, several administrations have managed to implement a combination of open-source and proprietary software, demonstrating that it is possible to find a balance that leverages the best of both worlds. Moreover, the existence of strong cybersecurity policies in many of these cities ensures that the transition to open technologies can be done securely, protecting critical systems from potential vulnerabilities.

Finally, progress is being made in implementing state initiatives that promote the use of open-source software, especially those aligned with national technology policies. These efforts, along with the growing participation of developers in collaborative events and projects, are laying the groundwork for a more inclusive and secure ecosystem in terms of technology and cybersecurity. While the challenges are considerable, the current context offers opportunities to transform how digital infrastructures are managed in the country's public entities.

Following the data collection and analysis phase, we remain focused on strengthening the use of open-source software and enhancing cybersecurity management. To address the challenges we've identified, we have decided to initiate our own open-source project. While there are existing open-source vulnerability scanners, many of them require advanced technical skills for configuration and may be overly complex or invasive for the needs of some organizations. In response, we propose a preventive vulnerability scanner that analyzes documentation related to digital infrastructure rather than directly scanning systems. We've named this tool the OSV Scanner (Open Source Vulnerabilities Scanner, https://github.com/titopuertolara/petiscanner).

The OSV Scanner aims to serve as a foundational tool for planning cybersecurity protocols and is not intended to replace robust vulnerability scanners. Instead, it offers an initial approach for organizations to identify potential vulnerabilities through their documentation. Our goal is to provide this tool as a free and collaborative resource, enabling organizations to improve their security posture without requiring extensive technical expertise.

OSV SCANNER

Despite the favorable perception of the security of open source systems, vulnerabilities persist in every deployment. Both open source and proprietary vulnerabilities are cataloged in the U.S. government's National Vulnerability Database. This database is updated regularly, providing risk assessments and severity ratings. For instance, the following figure illustrates the severity of vulnerabilities reported in the last month (August 2024) for three open source technologies: Apache, Linux, and PHP (Figure 9).

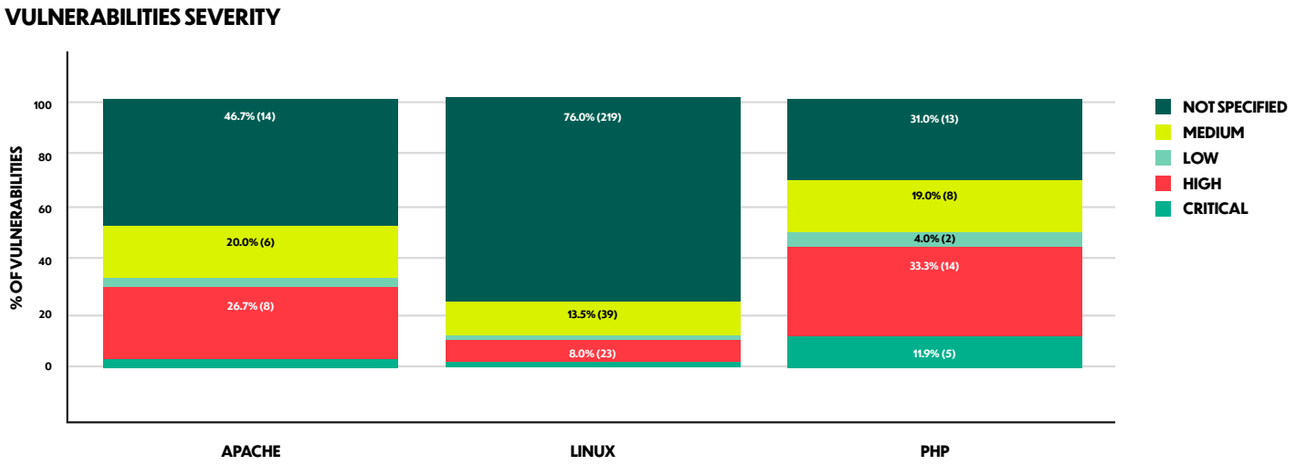


Figure 9 Vulnerabilities severity from the last month (source NVD)

In this previous plot, it is evident that a technology like Linux, renowned for its robust security, had over 200 vulnerabilities reported in the last month. Consequently, it is imperative for every IT department to conduct regular vulnerability scans of their systems. This proactive measure helps address and mitigate these vulnerabilities, thereby minimizing the risk of cyberattacks.

The most current vulnerability scanner softwares require installation, making them extremely invasive due to the need for complete system access to achieve their objectives.

To address this, we leveraged the NVD API to develop a non-invasive, online scanning tool. This tool uses a PDF file (e.g., Strategic Information Technology Plan or Digital Infrastructure official document) as input.

By analyzing the digital infrastructure detailed in each user's document, the tool collects vulnerabilities reported in the last month according to the technologies mentioned in those documents.

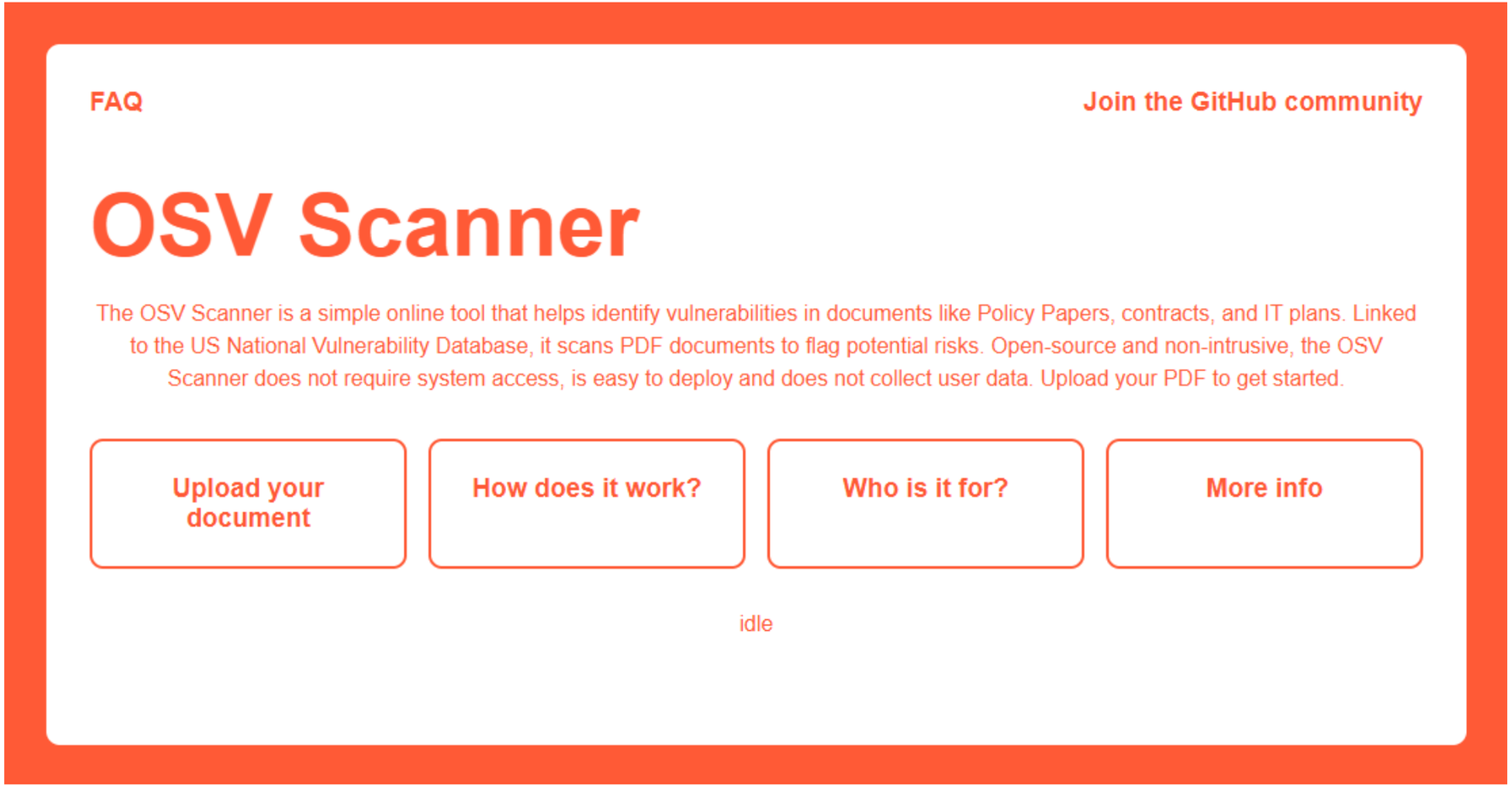


Figure 10. Open source vulnerabilities scanning tool

This tool provides statistics on the vulnerability status of each open source tool over the past month, including their respective severity levels. Additionally, it generates a structured database with each vulnerability indexed.

MAIN ADVANTAGES OF THE DEVELOPED TOOL

➔ **NON-INVASIVE OPERATION:** Unlike most current vulnerability scanning softwares that require installation on the operating system and full system access., our tool operates online, making it non-invasive and less disruptive to existing system operations.

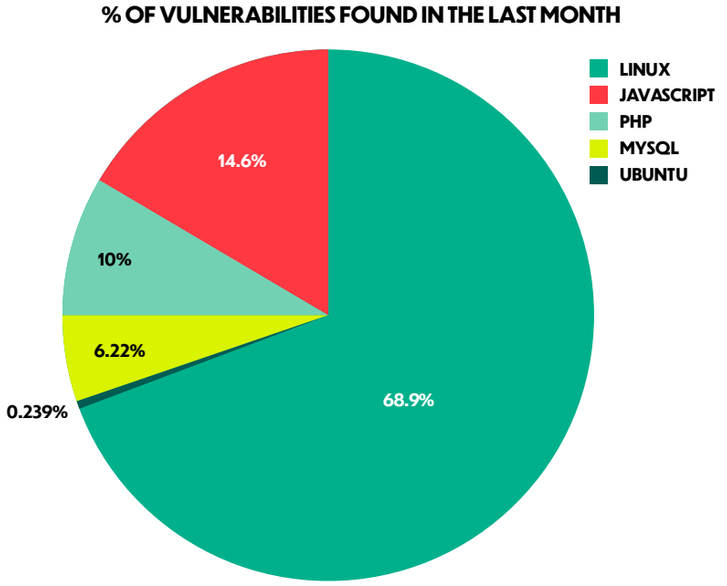
➔ **EASE OF USE:** The tool uses readily available PDF documents, such as Strategic Information Technology Plans or Digital Infrastructure official documents, as input. This approach simplifies the process of scanning for vulnerabilities without requiring complex setup or integration.

➔ **UP-TO-DATE VULNERABILITY DATA:** By leveraging the NVD API, the tool ensures that the vulnerability data is current, focusing on vulnerabilities reported in the last month. This timely information is crucial for maintaining system security.

➔ **STATISTICS AND SEVERITY LEVELS:** The tool provides comprehensive statistics on the vulnerability status of each open source tool, including detailed severity levels. This information helps users prioritize their security efforts based on the risk level of each vulnerability. (Figures 12.1 and 12.2)

➔ **STRUCTURED DATABASE:** The tool generates a structured database with each vulnerability indexed. This organized approach allows for easy reference and management of vulnerabilities, facilitating more efficient tracking and mitigation efforts. (Figure 13)

Figure 12.1 Statistics provided by OSV tool



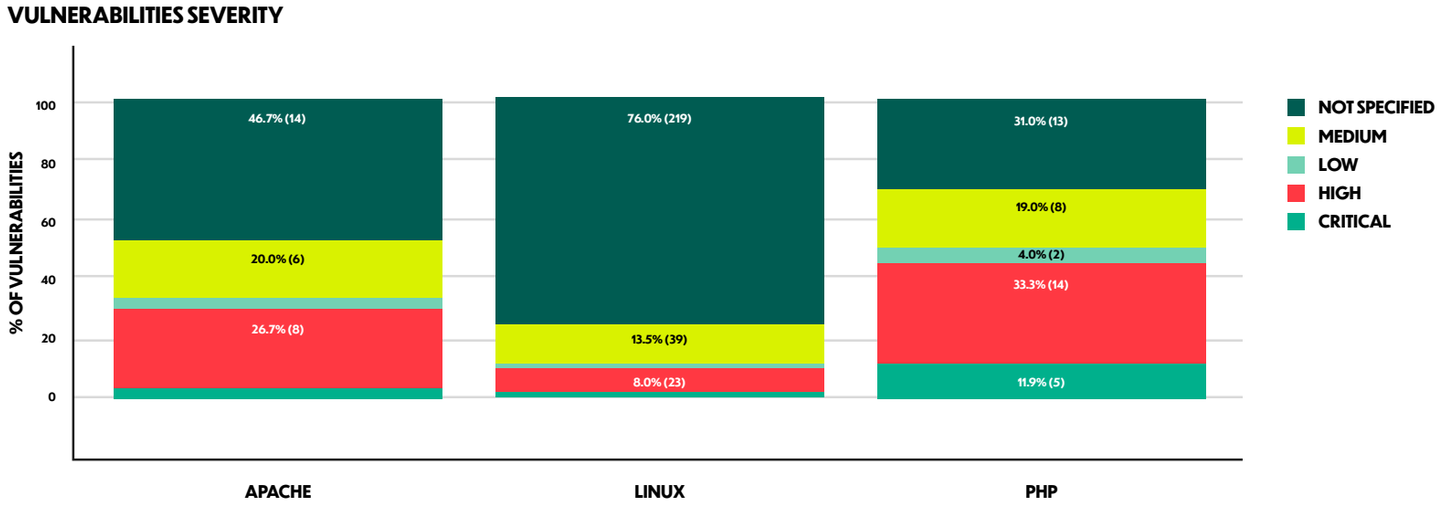


Figure 12.2 Statistics provided by OSV tool

Export

Id	Date	Contributor	Vulnerability	Severity	Tool
filter data...					
CVE-2024-45709	2024-12-10T09:15:06.013	psirt@solarwinds.com	SolarWinds Web Help ...	MEDIUM	linux
CVE-2024-41762	2024-12-07T14:15:17.560	psirt@us.ibm.com	IBM Db2 for Linux, UNI...	MEDIUM	linux
CVE-2024-37071	2024-12-07T13:15:04.047	psirt@us.ibm.com	IBM Db2 for Linux, UNI...	MEDIUM	linux
CVE-2024-53143	2024-12-07T07:15:03.780	416baaa9-dc9f-4396-8d...	In the Linux kernel, the f...		linux
CVE-2024-0139	2024-12-06T20:15:23.763	psirt@nvidia.com	NVIDIA Base Comman...	MEDIUM	linux
CVE-2024-12254	2024-12-06T16:15:20.623	cna@python.org	Starting in Python 3.12....	HIGH	linux
CVE-2024-53142	2024-12-06T10:15:06.203	416baaa9-dc9f-4396-8d...	In the Linux kernel, the f...	HIGH	linux
CVE-2024-53141	2024-12-06T10:15:06.050	416baaa9-dc9f-4396-8d...	In the Linux kernel, the f...	HIGH	linux
CVE-2024-51554	2024-12-05T13:15:08.843	cybersecurity@ch.abb.c...	Default Credentail vulne...	HIGH	linux
CVE-2024-51551	2024-12-05T13:15:08.700	cybersecurity@ch.abb.c...	Default Credentail vulne...	CRITICAL	linux
CVE-2024-51550	2024-12-05T13:15:08.543	cybersecurity@ch.abb.c...	Data Validation / Data S...	CRITICAL	linux

Figure 13. Sample of structure table for further analysis

CONCLUSIONS

Municipal authorities in Colombia are increasingly adopting open-source software (OSS) to enhance governance, public services, and public safety. While OSS usage is growing reported by 47% of departments and 56% of capital citie significant challenges remain. Larger cities like Bogotá and Medellín, with greater resources, are leading the change in OSS adoption and strategic integration. In contrast, smaller municipalities face financial and technical barriers that limit their ability to fully utilize OSS.

Key obstacles hindering OSS adoption and cybersecurity readyness include a shortage of skilled personnel, outdated procurement regulations, inadequate cybersecurity resources, and cultural resistance within organizations. Municipalities are required to develop their own IT plans (PETIs), often constrained by limited budgets and shifting political priorities, making it harder to address vulnerabilities effectively. Additionally, delayed access to information about security threats, slow vulnerability patching processes, and inconsistent enforcement of policies exacerbate these issues, leaving cities exposed to cyberattacks.

Despite these challenges, OSS offers significant potential to improve governance and public service delivery. Its open nature fosters innovation, collaboration, and quicker responses to vulnerabilities. To unlock this potential, a unified national cybersecurity strategy, greater investment in IT training, modernization of procurement policies, and a cultural shift that values OSS are crucial.

Finally, and in the meantime, there is an urgent call to action to strengthen municipal governments' cybersecurity readiness. One key step is deploying the OSV scanner we developed, which provides local governments with real-time information on cybersecurity threats and vulnerabilities as they are reported to the CISA bulletin. This tool can help cities stay ahead of emerging threats, improve their response times, and mitigate risks, laying a strong foundation for secure and efficient governance through OSS.

WORKS CITED

Ajuntament de Barcelona. "Free Software management." barcelona.cat, 2017, https://www.barcelona.cat/digitalstandards/es/free-soft/0.2/introduction. Accessed 18 May 2024.

Copeland, Eddie. Small pieces loosely joined: How smarter use of technology and data can deliver real reform of local government? Report. London, Policy Exchange, 2015, https://policyexchange.org.uk/publication/small-pieces-loosely-joined-how-smarter-use-of-technology-and-data-can-deliver-real-reform-of-local-government/.

European commision. OPEN SOURCE SOFTWARE STRATEGY 2020 – 2023. 2020, https://commission.europa.eu/document/download/97e59978-42c0-4b4a-9406-8f1a86837530_en?filename=en_ec_open_source_strategy_2020-2023.pdf.

Gobierno Digital. "Base de datos de Entidades Nacionales de la Rama Ejecutiva haciendo uso de software libre- Meta ASPA." datos.gov.co, 2024, https://www.datos.gov.co/Ciencia-Tecnolog-a-e-Innovaci-n/Base-de-datos-de-Entidades-Nacionales-de-la-Rama-E/huc3-sbgp/about_data. Accessed 22 May 2024.

Hoffman, Manuel, et al. The Value of Open Source Software. Working paper. no. 24-038, 1 January 2024. Harvard Business School, Harvard Business School, https://www.hbs.edu/ris/Publication%20Files/24-038_51f8444f-502c-4139-8bf2-56eb4b65c58a.pdf.

Kingsbury, Benedict, et al. OSS as Digital Infrastructure: Legal Technologies & Institutional Design. Project One-pager. 2021, https://www.fordfoundation.org/wp-content/uploads/2020/12/nyu_ford-sloan-one-pager.pdf.

Sharma, Chinmayi. "Tragedy of the Digital Commons." North Carolina Law Review, 2023, https://scholarship.law.unc.edu/nclr/vol101/iss4/6/.

Synopsys. 2024 Open Source Security and Risk Analysis Report. Report. 9th ed., 27 February 2024. Synopsys, Synopys, https://www.synopsys.com/software-integrity/resources/analyst-reports/open-source-security-risk-analysis.html.

Thévenet, Axel, et al. Open Source Software Country Intelligence Report, The Netherlands. 2023, https://joinup.ec.europa.eu/sites/default/files/inline-files/Open%20Source%20Software%20Country%20Intelligence%20Report%20-%20The%20Netherlands.pdf.

Wachs, Johannes, et al. "The Geography of Open Source Software: Evidence from GitHub." Technological Forecasting & Social Change, 2022.

White House. SECURING THE OPEN-SOURCE SOFTWARE ECOSYSTEM JANUARY 2024 END OF YEAR REPORT: OPEN-SOURCE SOFTWARE SECURITY INITIATIVE. 2024, https://www.whitehouse.gov/wp-content/uploads/2024/01/Securing-the-Open-Source-Software-Ecosystem-OS3I-End-of-Year-Report-MASTERCOPY.pdf.

Zárate Botía, C. G., & Peña Márquez, J. C. (2014). Plan Estratégico Departamental de Ciencia, Tecnología e Innovación (PEDCTI) – Departamento del Vaupés.

Gobernación del Vaupés; Universidad Nacional de Colombia Sede Amazonia, Instituto Amazónico de Investigaciones – IMANI. ISBN: 978-958-775-003-4.

Gobernación de Antioquia. (5 de Febrero de 2024). Gobernación de Antioquia. Obtenido de Gobernación de Antioquia : https://antioquia.gov.co/images/PDF2/Transparencia/2024/02/peti-2024-2027.pdf

Dirección de las Tecnologías y las Comunicaciones - Gobernación de Bolivar. (Diciembre de 2023).

Aruca, G. d. (16 de Junio de 2023). Gobernación de Arauca. Obtenido de https://arauca.gov.co/wpfd_file/plan-estrategico-de-las-tecnologias-peti-v1-2023-con-firmas/

Gobernación del Atlántico. (31 de Enero de 2023). Gobernación del Atlántico. Obtenido de https://www.atlantico.gov.co/index.php/listado-general-de-planes/664-plan-estrategico-de-ti-peti/23083-plan-estrategico-de-ti-peti-2022-2023-actualizacion

Gobernación de Boyacá. (23 de Enero de 2024). Gobernación de Boyacá. Obtenido de https://www.boyaca.gov.co/wp-content/uploads/2024/01/10.-PlanEstrategicoPETI_2024_Revision.pdf

Gobernación de Caldas. (31 de Enero de 2023). Gobernación de Caldas. Obtenido de https://site.caldas.gov.co/10-modelo-integrado-de-planeacion-y-gestion/512-2023/3073-petic-2020-2023-gobernacion-de-caldas-pdf

Gobernanción De Santander. (19 de Mayo de 2021). Gobernación de Santander. Obtenido de https://santander.gov.co/publicaciones/7076/plan-estrategico-de-tecnologias-de-la-informacion-y-las-comunicaciones-peti-2020-2023/

Gobernación del Tolima. (1 de Mayo de 2021). Obtenido de https://www.tolima.gov.co/gobernacion/nosotros/mision-y-vision/144-gobernacion/gobierno-digital/2341-plan-peti#1989-vigencia-2021

Gobernación de Caquetá. (02 de Diciembre de 2020). Gobernación de Caquetá. Obtenido de https://caqueta.micolombiadigital.gov.co/sites/caqueta/content/files/001264/63184_peti-2021-gobernacion-del-caqueta.pdf

Gobernación del Casanare. (2020). Gobernación de Casanare.

Gobernacion del Cauca. (30 de Diciembre de 2021). Gobernación de Cauca. Obtenido de https://www.cauca.gov.co/NuestraGestion/PlaneacionGestionyControl/Plan%20Estrat%C3%A9gico%20de%20Tecnolog%C3%ADas%20de%20Informaci%C3%B3n%20PETI%202022.pdf

Valledupar, G. d. (26 de Noviembre de 2022). Gobernación del Cesar. Obtenido de https://www.cesar.gov.co/d/index.php/es/menvertpolpla/menvertplanmipg/2816-artmainmenpolyplamipgpeti

Gobernación de Cundinamarca. (31 de Enero de 2024). Gobernación de Cundinamarca. Obtenido de https://www.cundinamarca.gov.co/dependencias/sectic/transparencia/petic

Gobernación del Guinía. (3 de Marzo de 2020). Gobernación del Guainía. Obtenido de https://www.guainia.gov.co/planes/peti-20202023

Gobernación Guviare. (31 de Enero de 2022). Gobernación de Guaviare. Obtenido de https://www.guaviare.gov.co/planes/peti-2020--2023-gobernacion-guaviare-ver-21

Gobernación del Huila. (Enero de 2020). Obtenido de https://www.huila.gov.co/documentos/1362/plan-estrategico-de-tecnologias-de-la-informacion/

Gobernación del Magdalena. (31 de Enero de 2023). Gobernación del Magdalena. Obtenido de Gobernación del Magdalena : https://www.gobernaciondelmagdalena.gov.co/plan-estrategico-de-tecnologias-de-la-informacion-2022-2023/

Gobernación del Meta. (6 de Junio de 2023). Obtenido de https://meta.gov.co/pagina/plan-estrategico-de-tecnologias-de-la-informacion-peti/56

Gobernación del Meta. (Enero de 2022). Gobernación del Meta. Obtenido de https://2020-2023.narino.gov.co/wp-content/uploads/2022/01/plan-Estrategico-de-tecnologia.pdf

Gobernación de Nariño. (Enero de 2023). Gobernación de Nariño. Obtenido de https://2020-2023.narino.gov.co/wp-content/uploads/2023/02/Plan-Estrategico-de-Tecnologia-de-Informacion-y-Comunicacion-PETI-version-2.0.pdf

Gobernación de Norte de Santander. (2022). Gobernación de Norte de Santander. Obtenido de https://administrador.nortedesantander.gov.co/wp-content/uploads/2022/12/PETI_2020_2023_FASES_III_y_IV_CONSTRUCCION_.pdf

Gobernación Putumayo. (29 de Junio de 2018). Gobernación Putumayo. Obtenido de https://www.putumayo.gov.co/images/documentos/Planes_y_programas/PLAN%20ESTRATGICO%20INFORMTICO_V4b%202020.pdf

Gobernación de Vichada. (31 de Enero de 2023). Gobernación de Vichada. Obtenido de http://www.vichada.gov.co/planes/peti--gobernacion-de-vichada

Gobernación del Quindio. (28 de Enero de 2022). Gobernación del Quindii. Obtenido de https://quindio.gov.co/medios/PL-TIC-03PETIV2.pdf

Departamento de Risaralda. (31 de Enero de 2024). Obtenido de Departamento de Risaralda : https://www.risaralda.gov.co/documentos/150100/peti/

Gobernación del Archipiélago de San Ándres, Providencia y Santa Catalina. (8 de Febrero de 2023). Obtenido de Gobernación del Archipiélago de San Ándres, Providencia y Santa Catalina : https://www.sanandres.gov.co/index.php/6-planeacion/c-plan-estrategico/plan-estrategico-de-tecnologias-de-la-informacion-y-las-comunicaciones-peti?own=0

Gobernación de Córdoba. (28 de Enero de 2021). Gobernación de Córdoba. Obtenido de https://www.cordoba.gov.co/documentos/529/peti/

Municipio de Armenia. (2022). Plan Estrategégico de Tecnoligías de la Información y las Comunicaciones -PETI. Armenia : Secretaría de Tecnolgías de la Información y las Comunicaciones.

Alcaldía de Barranquilla. (2024). Plan estratégico de tecnologías de la información- PETI 2024 -2027. Barranquilla : Alcaldía de Barranquilla.

Alcaldía Mayor de Bogotá D.C. (2022). Plan Estrategico de las Tecnologias de la información y Comunicaciones. Bogotá.

Alcaldia de Bucaramanga. (2024). Plan Estratrégico de Tecnologías de Información. Buracamanga.

Alcaldía Santiago de Cali. (2024). Plan Estratégico de Tecnologías de la Información y las comunicaciones 2024-2027. Cali.

Alcaldía Disteital de Cartagena de Indias. (2019). Plan Estratégico de Tecnologías de la Información. Cartagena : oficina Asesora de Informática.

Alcaldía de Florencia. (2021). Plan Estrategico de Tecnologias de la Información y las Comunicaciones PETI. Florencia.

Alcaldía de Ibagué. (2019). Plan Estratégico de Tecnologías de Información y Comunicaciones - PETIC. Ibagué.

Alcaldía de Leticia. (2022). Plan Estratégico de Tecnologías de la Información. Leticia.

Alcaldía de Manizales. (2022). Plan Estratégico de las Tecnologías de la Información. Manizales.

Alcaldía de Medellín. (2020). Plan Estratégico de las Tecnologías de la Información 2021 -2024. Medellín.

Alcaldía de Mitú. (2020). Plan Estratégico de Tecnologías de las información 2020-2023. Mitú.

Alcalcía de San José de Cúcuta. (2024). Plan Estrategico de Tecnologias de la Información y las Comunicaciones PETI. Cúcuta.

Alcaldía Municipal de Mocoa. (2020). Plan Estratégico de Tecnologías de la Información. Moccoa.

Alcaldía de Montería. (2024). Plan Estratégico de Tecnologías de la Información 2020 versión 4.0. Montería.

Alcaldía de Neiva. (2020). Plan Estratégico de Tecnologías de la Información y las Comunicaciones PETI. Neiva.

Alcaldía Municipal de Pasto. (2021). Plan Estratégico de Tecnologias de la Información y las Comunicaciones PETI. Pasto.

Alcaldía de Pereira. (2019). Plan Estrategico de Tecnologías de Información y Comunicaciones - PETIC. Pereira.

Alcaldía de Popayán. (2020). Plan Estratégico de Tecnologías de la Información 2021 -2024. Popayán.

Alcaldía de Quibdo. (2024). Plan Estratégico tecnologías de la Información 2024-2027. Quibdó.

Alcaldía del Municipio de San José del Guaviare. (2024). PETI Plan Estratégico de Tecnologías de Información. San José del Guaviaré.

Alcaldía de Santa Marta. (2022). Plan Estratégico de Tecnologías de la Información - PETI. Santa Marta.

Área Metropolitana de Valledupar. (2024). Plan Estratégico de Tecnologías de la Información y las Comunicaciones- PETI, de Riesgos de Seguridad y Privacidad de la Información del Área Metropolitana de Valledupar 2024. Valledupar.

Alcaldía de Yopal. (2018). Plan Estratégico de Tecnología - PETI. Yopal.

EDGELANDS

edgelands.institute