WITHOUT RIGHTS ON #INTERNETVE

Report on the situation of digital human rights in Venezuela

2022+2023 REPORT

VESINFILTRO.ORG/2022+2023

INTERNET ACCESS
CENSORSHIP AND BLOCKINGS
SURVEILLANCE AND PRIVACY
ACCESSIBILITY
DIGITAL ATTACKS
PERSONAL DATA

VE SIN FILTRO

VE SIN FILTRO

CONEXIÓN SEGURA Y LIBRE

About VE sin Filtro

VE sin Filtro is a program of Connexion Segura y Libre (Free and Secure Online) dedicated to monitoring and documenting threats to the exercise of human rights in the digital environment in Venezuela. Since 2014, it has helped to identify and evade censorship in the media and has been a pioneer in the joint use of automatically produced network measurements, volunteer contributions, and network traffic analysis to document internet censorship with technical criteria; and in the use open-source investigations to examine restrictions on human rights on the internet to attribute digital attacks to public entities in Venezuela.

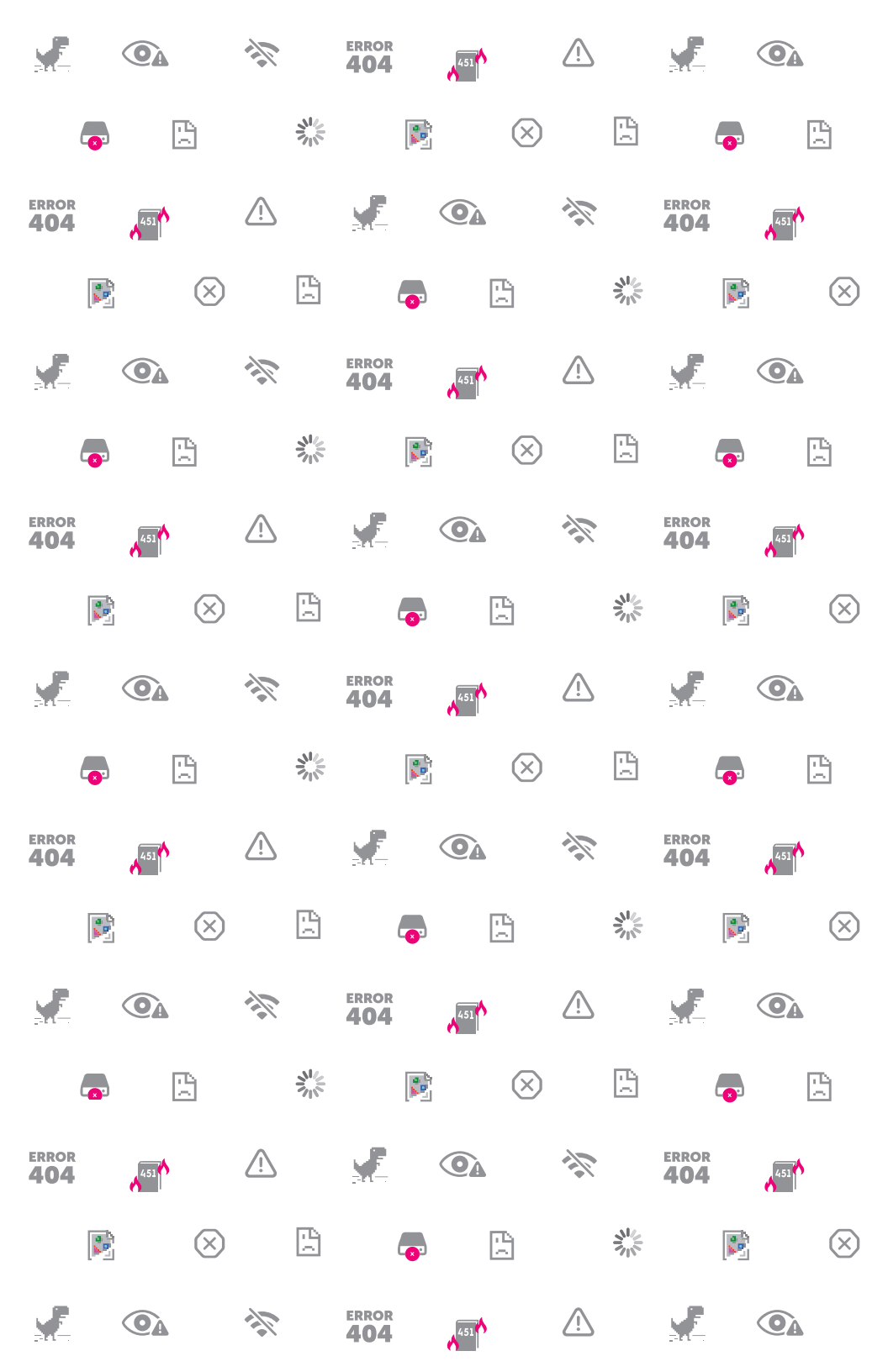
VE sin Filtro, along with the Conexión Segura program, offers emergency assistance to civil society organizations, journalists, and independent media under attack or recently blocked; helping to resolve the incident and mitigate the impact of censorship. With technical evidence and data analysis, it unveils and documents the extent of internet blockages and censorship, indiscriminate government surveillance, and cyberattacks against civil society.

Through constant monitoring, VE sin Filtro provides real-time updates on the state of the internet in Venezuela. This work not only focuses on connectivity and unequal internet access but also on tracking service interruptions, attacks, and internet blocks and shutdowns, with the aim of protecting access to information, freedom of expression, privacy, security, education, participation, among other fundamental rights.

VE sin Filtro offers support and training to activists, journalists, and organizations; it develops recommendations and prepares best practices to counter threats against their rights and security. The VE sin Filtro program won the Frida Award for a Free and Open Internet, awarded by LACNIC. Its work is considered in reports of other Human Rights organizations and has been cited by Time, The Washington Post, and El País.

The documentation of VE Sin Filtro has been fundamental for international organizations to denounce the Venezuelan state for the abusive use of its powers, for applying prior censorship against content of public interest, and for the lack of policies that guarantee equal access to the internet.

Index


ERROR
404
451

1 INTERNET ACCESS IN VENEZUELA

Internet access is considered a human right by the United Nations , allowing people to exercise their right to freedom of expression, access information and participate in social and economic activities.

In 2015, the United Nations established the Sustainable Development Goals (SDGs). One of the targets is to "significantly increase access to the Internet and information and communication technologies (ICTs) and strive to provide universal and affordable access to the Internet in the least developed countries by 2020."

Improving Internet access can also contribute to the achievement of other SDGs, such as reducing poverty, promoting economic growth and improving education and health. The United Nations Development Programme (UNDP) created the Multidimensional Poverty Index (MPI), which includes Internet access as one of its five key dimensions.

The International Telecommunication Union (ITU) estimated that a 10% increase in fixed broadband penetration could lead to a 1.57% increase in the regional Gross Domestic Product of Latin America and the Caribbean.

Internet connectivity is positively correlated with increased labor force participation, labor mobility, job creation and overall job growth. Internet access also strengthens economic and social resilience by facilitating access to essential public services such as education and healthcare, as well as to training and telecommuting opportunities.

Venezuela went from having a competitive and vibrant telecommunications ecosystem, compared to its peers, to having one of the worst Internet services in the world, which is just beginning to improve but in a very unequal manner, with the wealthier Venezuelans getting higher quality service and the less fortunate frequently stuck with insufficient access. The potential for widespread Internet access has been thwarted by economic and political crises that have negatively affected the development of meaningful Internet access.

Information sources covering Internet access in Venezuela tend to provide different figures due to different methodologies. For example, the National Telecommunications Commission (CONATEL), the national telecommunications regulator, does not publicly provide details on its methodologies, but has data on all Internet providers and subscribers to the service, and publishes outdated metrics.

Free, transparent and equitable access to data and information of public interest is essential for the analysis of the factors shaping the Internet in Venezuela, but access to public information is severely restricted and institutions often ignore requests for information. Transparencia Venezuela's

assessment of the Law on Transparency and Access to Information of Public Interest of 2021 is that, far from guaranteeing that right, it further consolidated secrecy.

Widespread restrictions on press freedom, including censorship and self-censorship, are forcing traditional media, such as newspapers and radio and television stations, out of the analog markets.

Similarly, with the virtual disappearance of independent newspapers, the disappearance of critical opinions and television news, the proliferation of censorship and the decrease in the number of independent radio stations, many citizens have turned to the Internet to stay informed. Internet access has thus become essential for the exercise of political and civil rights, despite the restrictions imposed by the government of Nicolás Maduro.

Venezuela's complex humanitarian crisis often makes Internet access necessary for those seeking information on the availability of scarce goods or services. These situations pose a risk to their physical safety, their migratory conditions and opportunities, and their ability to access public services and assistance.

1.1 Internet connection performance

Poor Internet quality can have negative effects on social conditions in Venezuela, particularly for members of vulnerable populations such as children, women, minorities (migrants, indigenous and others) and low-income people.

Some technical aspects related to quality that have a critical impact on online activities include:

Speed:
Is one of the most critical aspects of Internet quality, including both download and upload speed. Download speed refers to the speed at which data is transferred from the Internet to a device; upload speed is the speed at which data is transferred from a device to the Internet. Internet speed, also called bandwidth, is divided among users on the same network. Some activities, such as streaming video or music, require higher speeds than others, such as reading an article online.

Latency:
Refers to the time it takes for data to travel from one point in a network to another. It is usually measured in milliseconds. Lower latency means faster response times and a better experience, especially for real-time and interactive applications; higher latency can make many tasks impossible, especially video conferencing. Even voice-only meetings can be impossible on networks with high latency levels.

Packet loss:
Occurs when parts of the communication do not reach their destination while being transmitted over a network. High packet loss can result in

a poor user experience, such as choppy audio or video and delays or missing information.

In this context, children and young people miss out on quality educational and learning opportunities when they only have access to poor quality connections.

Similarly, low-income people may have difficulty meeting their basic needs or accessing social protection programs due to lack of access to online platforms, digital payments or the necessary identification systems. They may also fall behind in terms of income generation or employment opportunities due to lack of digital literacy or digital resources.

1.2 Internet penetration

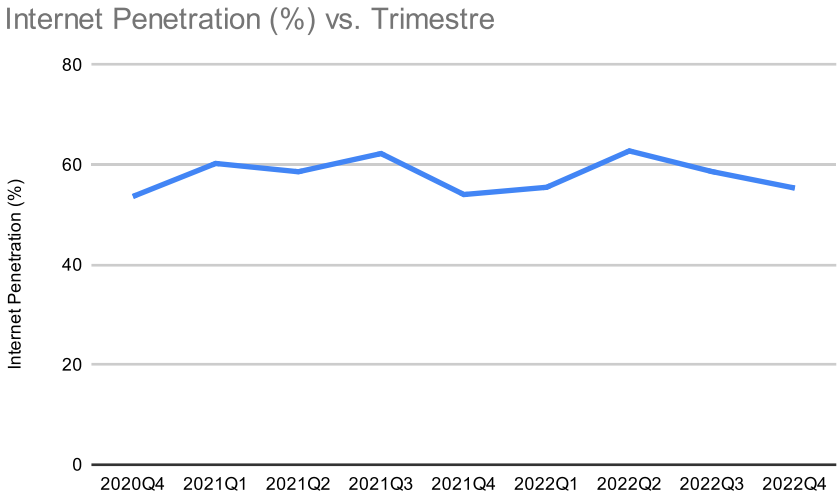
Since the Internet is an essential mediator for the exercise of human rights today, access to it is essential for full participation in society.

The Venezuelan Observatory of Public Services, in May 2022, estimated that 42.8% of the population had fixed Internet service[1], evidencing an increase of 8.6 percentage points between January 2021 and May 2022, while 87.5% had mobile Internet service in May 2022, which means an increase of 14.5 percentage points since January 2021.

Official sources of Internet penetration come from CONATEL, with a methodology that is not sufficiently documented. CONATEL reports a penetration of 55.34% at the end of 2022, an increase of 1.29 percentage points compared to the last quarter of 2021. If the figures for the year are averaged to reduce variations between quarters, 2022 on average had an Internet penetration 0.72 points lower than 2021.

These official Internet penetration figures count users with residential internet access along with others who only have access to mobile telephony and on data plans that are really insufficient for normal use, or cellular data often doesn't work well enough in their homes. Likewise, they seem to assume that all Internet service customers have a working connection, but a large number of CANTV customers have not had service for months or years. According to the Observatorio Venezolano de Servicios Públicos (OVSP), 41.2% of Venezuelans without Internet access say the reason is lack of service from CANTV. It is not clear whether respondents included places without coverage and those whose service was down for very long periods of time.

[1] https://www.observatoriovsp.org/wp-content/uploads/boletin-38_agosto-2022_primera-entrega-comprimido.pdf

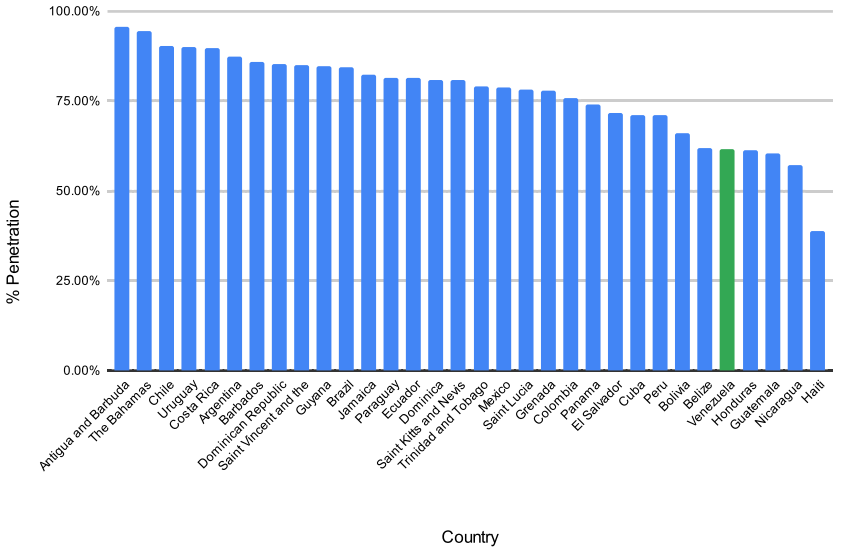


Graph of Internet penetration in Venezuela by quarter, based on using CONATEL's Internet penetration figures. (Source: VE sin Filtro, using CONATEL data).

According to the penetration rates published by Kepios in its first 2023 reports, Venezuela has one of the lowest Internet penetration rates in Latin America, ranking fifth. This rate is lower than the average for Latin America and the Caribbean, which is 76.64%. Increasing Internet penetration is crucial for economic development and social inclusion. Research has shown that increasing broadband Internet access has a positive impact on economic growth rates.

Penetration Rate in Latam 2023

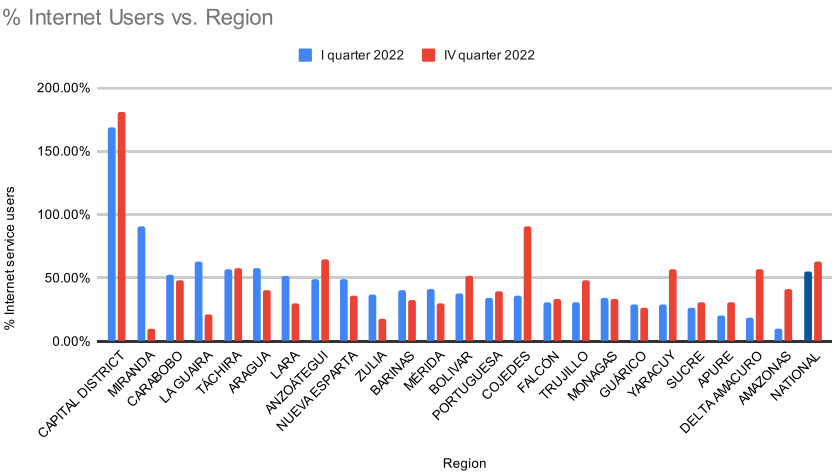
Source: Kepios



Bar chart showing penetration rate in Latin America based on Kepios data from its first publication in 2023. (Source: VE sin Filtro, using Kepios data).

Regarding the distribution of users, the CONATEL report corresponding to the first quarter of the year 2022, evidences the inequality in Internet access in the country, the 10 states with the lowest penetration (from lowest to highest) are Amazonas, Delta Amacuro, Apure, Sucre, Yaracuy, Guárico, Falcón, Trujillo, Monagas and Portuguesa. For the last quarter, the states of Falcón and Monagas changed position and Cojedes moved to the last place in this list, while the Distrito Capital and the state of Miranda have 167.34% and 90.22% of Internet penetration respectively.

By the end of 2022, the Distrito Capital and Miranda continued to be the states with the highest penetration, but Distrito Capital increased 30.36 percentage points, on the contrary Miranda decreased 2.24 points. CONATEL's undefined methodology for estimating the number of Internet service users could influence the penetration estimate for Distrito Capital (167.34%).



Bar chart of the percentage of Internet service users by state in Venezuela for the 1st and 4th quarters of 2022. (Source: VE sin Filtro, using CONATEL data).

This is evidence that there is a significant gap between rural and urban states in the country. States with higher penetration rates have higher population density. 22 of Venezuela's 24 states have unstable and unequal Internet access, which correlates positively with the country's population density.

One event that demonstrated the consequences of limited Internet access for physical security and the right to life was a confrontation in the municipality of Alto Orinoco, Amazonas state, on March 20, 2022, between Venezuelan military and members of an indigenous group. In the altercation, Venezuelan soldiers opened fire on a group of Yanomami after they asked them to share access to their Internet service, leaving four dead (one woman and three men) and five others wounded (including a 16-year-old boy).

1.3 Internet speed

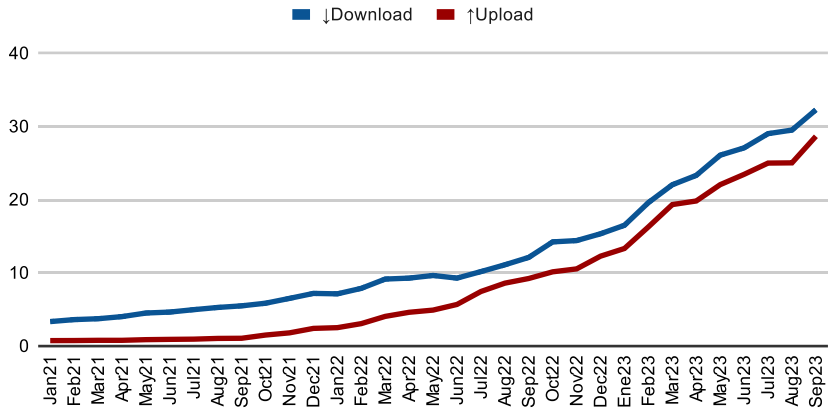
Internet speed can be an obstacle to its use and can be affected by multiple factors. There are several ways to measure Internet speed, and they are not always comparable. Some major sources, such as the network testing company Ookla, can be biased because they do not use a random sample of connections from across the country; instead, they use voluntary information from individuals, often more tech-savvy, who, for example, can provide speed measurements using the tool to determine the speed of their connection.

In Venezuela, the average fixed Internet speed is 16.5 Mbps for download, the second slowest in Latin America. It ranks behind Cuba, with 1.84 Mbps for download according to the Global Speedtest Index of network testing company Ookla (as of January 2023). At the opposite extreme, Chile has

the highest average download speed in the region (224.84 Mbps) and the second fastest in the world. Similarly, Venezuela's average upload speed of 13.33 Mbps is ten times slower than Chile's (133.81 Mbps). Venezuela ranks 138th out of the 179 countries included in Ookla's sample.

Fixed Internet Speed (2021-2023)

Fuente: Venezuela's Fixed Broadband Internet Speeds - Ookla

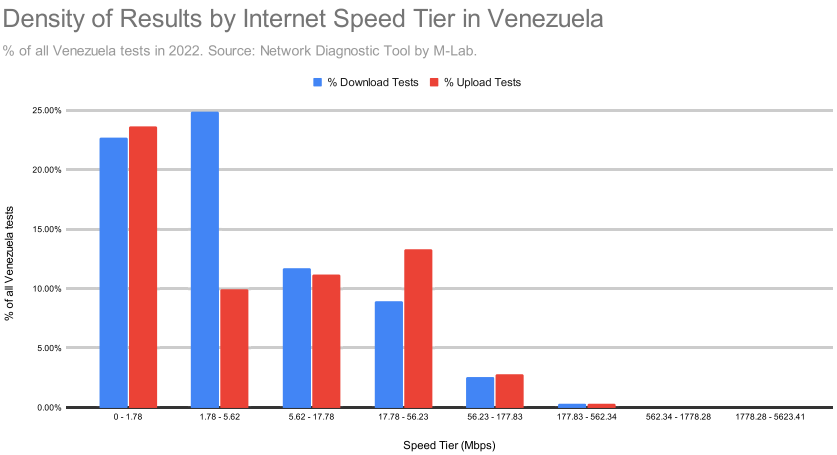


Graph of fixed broadband Internet upload and download speeds from 2021 to the third quarter of 2023. (Source: VE sin Filtro, using Ookla data).

Compared to OOKLA's 2022 figures, the median download speed during January 2022 was 7.13 Mbps, which means that there was an increase of 131.4%. The upload was 2.51 Mbps (January 2022), in this case the increase experienced during 2022 was 431.1%.

M-Lab, a project with partners from civil society, educational institutions and the private sector, uses a different methodology that focuses on the speed of a single communication thread between your device and a server. This is more accurate for the quality of the network effect on single applications, whereas the multi-threaded approach that comes by default in the Ookla speed test is more accurate for maximum bandwidth when saturated by multiple applications or multi-threaded applications, such as video streaming. There are also selection biases introduced by the source of each measurement.

M-lab places the median Internet speed in Venezuela between 1.02 and 5.21 Mbps download and between 1.63 and 4.29 Mbps upload, during January 2022 and January 2023, using its single-threaded traffic test. M-Lab's methodology better represents the performance of the connection for single demanding tasks, but the speed figures are lower than what would be expected in many real cases, where there are multiple simultaneous downloads.



Bar chart of the distribution of speed test results in Venezuela by speed range during calendar year 2022 using Network Diagnostics Tool measurements (Source: VE sin Filtro, using M-Lab data).

The M-lab figures clearly show that 22.7% and 24.9% of the download speed tests are between the 0 - 1.78 Mbps and 1.78 - 5.62 Mbps ranges respectively, while with respect to the upload speed test results, 23.6% are in the 0 - 1.78 Mbps range.

According to these measurements made with M-Lab's Network Diagnostic Tool, during 2022, at least 59% of Internet users in Venezuela still have insufficient broadband connections, which limits or prevents users from fully developing certain activities. Despite the recent increase in median speeds, it is important to keep in mind that the median speed is the point at which half of the users have a lower speed and the rest of the sample enjoys much higher connection speeds. This means that many Internet users with residential connections have trouble accessing the necessary services and exercising their online rights, not to mention people who do not have Internet access at home or rely exclusively on mobile Internet through prepaid cellular plans.

1.4 Offer

The technologies currently available in the ISP market offering are mainly Digital Subscriber Lines (DSL), coaxial cable, fiber optics, radio frequency and microwave.

According to VE sin Filtro's analysis of Internet service offerings for the first quarter of 2023, by researching Internet service plan offerings and prices, 60.53% are fiber optic plans, followed by radio frequency (19.3%), coaxial cable (8.77), DSL (6.14) and microwave (5.26). The technology with the largest number of users is DSL, with 2.2 million users, followed by cable modem (210,000 users), fiber to the home/building (67,000),

terrestrial fixed wireless (10,000), other fixed broadband (2,000) and satellite broadband (25).

Regarding demand, according to data from the last monitoring report of the Observatorio Social Humanitario of December 2022[2], in the last four months of the year there were between 54.5% and 57.2% of users at national level with Internet service through CANTV, 32.95% and 30.19% of users with fiber optic Internet through a private provider, while Internet users through a "satellite" service (radio frequency or microwave) were between 4.31% and 5.21%, as for users who do not have Internet service, they registered between 6.72% and 7.39%.

In terms of the speed of the available internet service plans, 60.5% of them have speeds equal to or higher than 30 Mbps. Of these, 84% are delivered using optical fiber and the rest use radio frequency or coaxial cable.

Plans with speeds below 30 Mbps primarily use DSL, radio frequency, microwave or coaxial cable technology, while all plans above 100 Mbps use fiber optics.

1.5 Cost

An analysis of the service packages of 24 national ISPs carried out from January to March 2023 shows the high cost of services, which is an obstacle to Internet access for Venezuelans. **The 115 plans analyzed show prices ranging from 0.08 to 56.22 times the monthly minimum wage, or from USD 0.41 (for a small cellphone data plan per consumption) to USD 300 (for fiber optic plans with 1Gbps speed).**

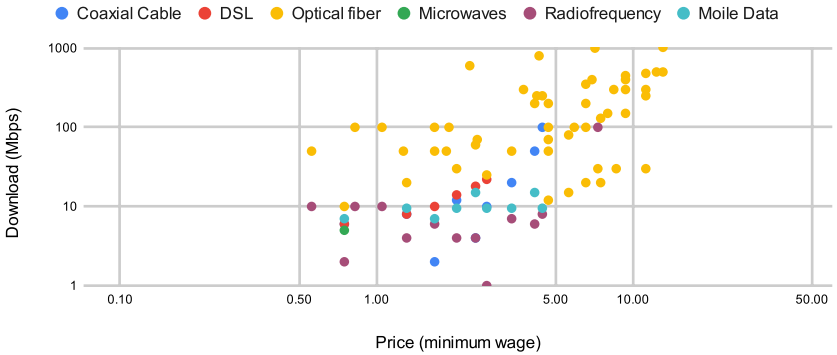
In this price range, the distribution of available plans is not even. There are 26 plans that cost between 4.44 and 6.93 times the minimum monthly salary, representing 22.6% of the plans analyzed. And 70.4% (81 plans) of the plans offered have prices between 4.44 and 56.22 times the minimum monthly salary.

The average price of the Internet packages reviewed was 6.93 times the monthly minimum wage; although this does not reflect the average expenditure on Internet access, it shows how much of the market is focused on the high end, leaving few affordable options for those earning lower incomes.

[2] Humanitarian Social Observatory (2023). Community Monitoring of Public Services. Report 4: Evaluation of the existence, quality and performance of public services in Venezuela. Observatorio Social Humanitario.

Offer of Internet Service Plans

Source: Ve Sin Filtro



Scatter plot of Internet service plans in Venezuela by download speed and price as a function of the Venezuelan minimum monthly salary in 2022.

The inflation that Venezuela has experienced in recent years has significantly decreased the purchasing power of a large portion of Venezuelans. The fact that only 13.27% of Internet service plans are priced at less than one minimum monthly wage is troubling in that the lack of affordable, high-quality options presents, along with the general lack of infrastructure in areas that have long been without reliable service or any service at all, one of the biggest barriers to Internet access. Ten of these thirteen plans are mobile data plans with data usage limits ranging from 50 MB to 10 GB per month.

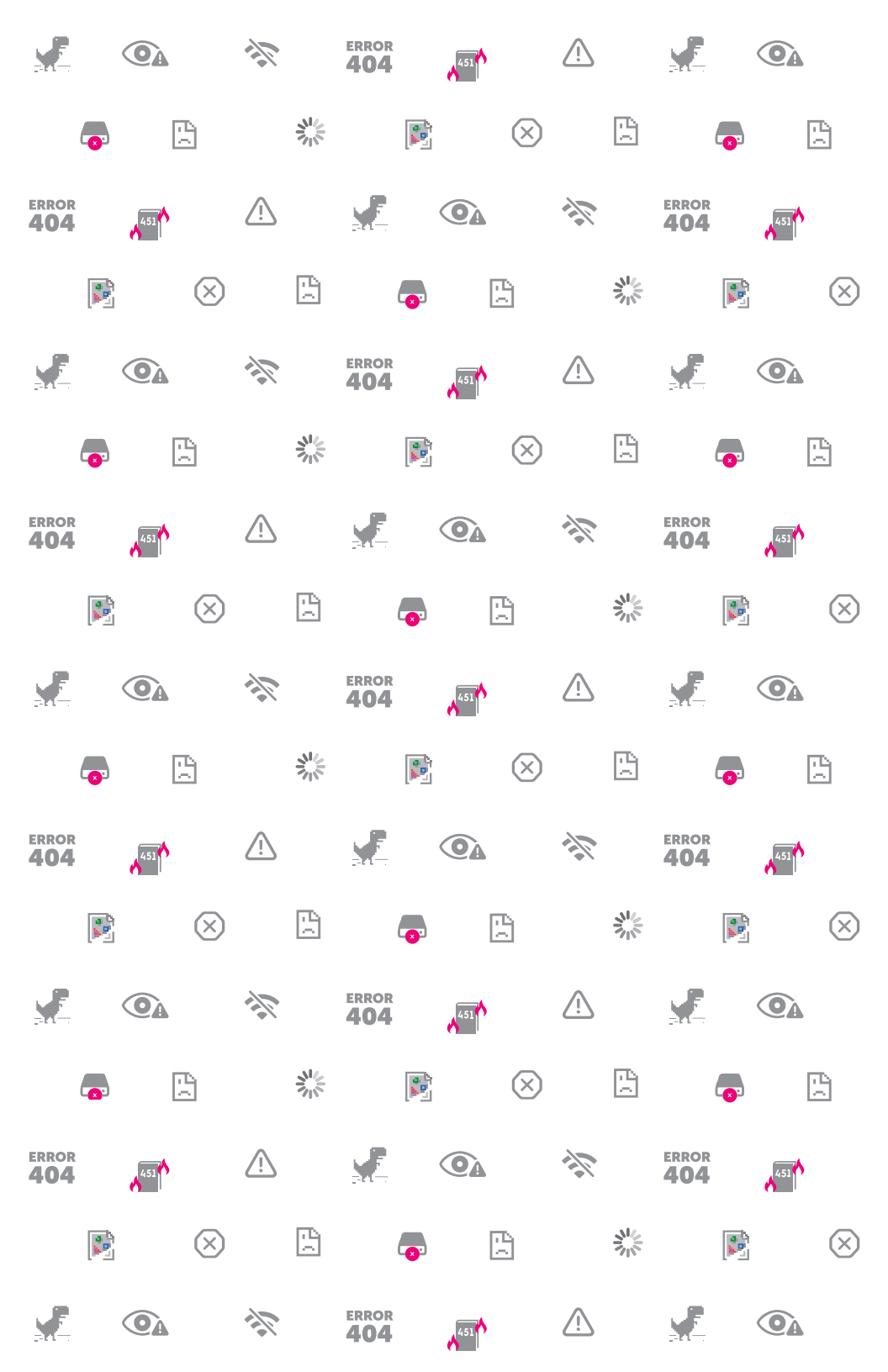
1.6 Geographic Distribution

Regarding the geographic distribution of Internet service offerings, the uneven distribution in the different states and other territories of the country is relevant: while half of the ISPs offer services in Caracas, most places have few or no options. Miranda has the second highest level of service, with eight ISPs, followed by Zulia (six) and Carabobo (five). There is a strong positive correlation with population density, as the states with the most limited offerings are also those with the lowest penetration rates, namely Amazonas, Anzoátegui, Apure, Cojedes, Guárico, Mérida, Portuguesa, Sucre, Táchira, Yaracuy and Delta Amacuro.

In some border states, ISPs take advantage of the proximity of the border and some citizens use wireless services from the neighboring country to access the Internet. Telecommunications journalist, William Peña, stated that some ISPs hire providers from neighboring countries to reduce costs and offer better bandwidth or lower prices, such as many offered in Zulia, some which connect to the Internet through Colombian providers.

The president of the Venezuelan Chamber of Telecommunication Services Companies (Casetel), Pedro Marín, has explained that one of the reasons why most ISPs serve only a few major cities[3], mainly Caracas, Maracaibo, Barquisimeto and Valencia, is the high cost of using the "Vías Generales de Telecomunicaciones", a common part of the physical infrastructure used by telecommunications networks that is owned and managed by state-owned companies in Venezuela.

[3] Díaz, Z. (2023, January 27). Deficiencias de Cantv dan paso al Internet de fibra óptica en zonas populares de Caracas. TalCual. https://talcualdigital.com/fallas-de-cantv-dieron-paso-al-Internet-de-fibra-optica-en-zonas-populares-de-caracas/


ERROR
404
451

2 CENSORSHIP THROUGH INTERNET BLOCKS

In Venezuela, access to information is crucial due to the complex social dynamics the country is experiencing. Censorship in traditional media and the global growth of the Internet make access to the network essential for the exercise of civil and political rights.

The Venezuelan government blocks websites as a censorship tactic. Several types of blocks have been identified: DNS, HTTP/HTTPS and TCP/IP. Private ISPs use DNS blocks and CANTV uses HTTP/HTTPS and DNS blocks. Each block affects user connections differently.

Blocking events:
Blocking events are mainly documented as events, to avoid the ambiguity that can exist when different blocking actions affect the same Internet service. The term “blocking event" refers to the blocking of a URL, domain, or IP address, using a specific blocking technique and by a particular ISP.

For example: the URL "caraotadigital.xyz" belonging to the website of the news media Caraota Digital, presents 7 blocking events, these are 6 DNS type blocks in the ISPs CANTV, Digitel, Movistar, Inter, Net Uno and Supercable, and one HTTP block in CANTV, for a total of 7 blocking events registered in the same **case.**

Blocking Cases:
Alternatively, all blocking events against the same service or website are considered as one case, which groups together blocking events from different domains. That is, each form of censorship implemented by different ISPs.

Most of the documented blocks are of the DNS type. With this type of blocking, ISPs reconfigure their Domain Name System (DNS) servers, which translate domain names into Internet addresses (IP addresses). This reconfiguration causes the servers to respond incorrectly to requests for the domains of the websites or other online services they aim to block. This practice is relatively simple and incurs no additional cost for the Internet operators that implement it.

Meanwhile, **HTTP and HTTPS blocking affects the content of Internet connections at multiple layers of the process, with equipment specially designed to examine each communication** for specific elements in Internet packets, such as the host name of the website, the requested URL, keywords in the body of the website or the Server Name Indication (SNI) to verify whether it should be blocked in what is called "Deep Packet

Inspection" (DPI). As a result, the HTTP/HTTPS blocking forces the user to use tools such as Tor or a VPN to circumvent censorship.

2.1 Internet blocks in 2022

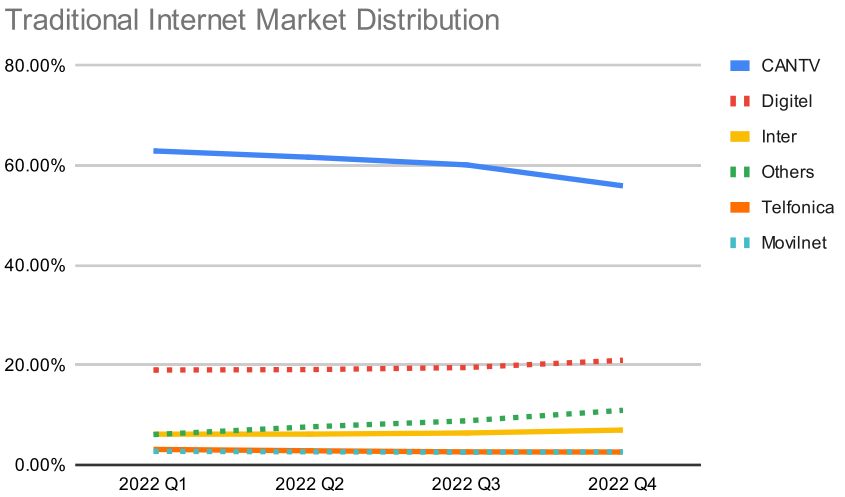
VE sin Filtro identified in 2022 more than 108 blocked URLs in Venezuela, including independent news sites. This limits freedom of expression and access to information.

CATEGORY	ABBREVIATION	CASES OF BLOCKED WEBSITES	BLOCKED URLS OR DOMAINS	TOTAL BLOCKING EVENTS
E-commerce	COMM	1	3	21
Economics	ECON	2	4	25
Hate Speech	HATE	1	1	6
Human Rights Issues	HUMR	4	4	16
Media Sharing	MMED	3	3	16
News Media	NEWS	43	66	336
Political Criticism	POLR	12	12	54
Pornography	PORN	8	8	21
Public Health	PUBH	2	2	8
Anonymization and circumvention tools	VPN	3	5	26
TOTAL YEAR 2022		77	108	529

Table showing the number of blocked websites, blocked urls or domains and blocking events by category recorded in 2022.

Blocking extends beyond the news media; in particular, this censorship is also applied against sites dedicated to political criticism, activism and sites with human rights content. All the main ISPs examined apply Internet blocking, including both public and private companies: CANTV, Movistar, Inter, Digitel, Net Uno and Supercable are the providers with the highest percentage of market share according to Conatel[4][5][6][7].

[4] Conatel. REPORT ON THE FIGURES OF THE Telecommunications SECTOR I QUARTER 2022 (second version published)
[5] Conatel. Telecommunications SECTOR FIGURES REPORT II QUARTER 2022
[6] Conatel. Telecommunications SECTOR FIGURES REPORT III QUARTER 2022
[7] Conatel. Telecommunications SECTOR FIGURES REPORT IV QUARTER 2022



Graph of the ISP market share, including residential and mobile providers, in Venezuela during the year 2022, determined using CONATEL's internet penetration figures. (Source: VE sin Filtro via CONATEL)

The Internet blocks not only affect the freedom of information of citizens in Venezuela, but are also an obstacle to education and access to quality information for students and researchers, as well as the right to freedom of association, political participation and the development of work activities, among many others.

The blocking of websites in Venezuela does not conform to international human rights standards. These blocks are ordered ex officio, at the discretion of CONATEL, lacking transparency and a clear legal basis. The implementation of these internet blocking orders occurs without due

process guarantees and is not supervised or authorized by a judicial authority.

SITE	DOMAIN	CATEGORY	CANTV	Movistar	Digitel	Inter	NetUno	Super Cable
2001	www.2001.com.ve	NEWS	HTTP+DNS	No	No	No	No	No
6th power	6topoder.com	NEWS	DNS	DNS	DNS	DNS	DNS	DNS
Aguacateverde.com	www.aguacateverde.com	NEWS	HTTP+DNS	DNS	DNS	No	DNS	DNS
To the ship	alnavio.com	NEWS	HTTP+DNS	DNS	DNS	DNS	DNS	DNS
Alberto News	albertonews.com	NEWS	HTTP+DNS	DNS	DNS	DNS	DNS	No
Alberto News	awsveanews.com	NEWS	HTTP	No	No	No	No	No
Alberto News	b1tly4n3s.com	NEWS	HTTP	No	No	No	No	No
Alberto News	www.b1tlydns02io.com	NEWS	HTTP	No	No	No	No	No
Alek boyd	alekboyd.blogspot.co.uk	NEWS	HTTP+DNS	DNS	DNS	No	DNS	DNS
Alek boyd	alekboyd.blogspot.com	NEWS	No	DNS	DNS	No	DNS	DNS
Analysis 24	analisis24.com	NEWS	No	DNS	No	DNS	DNS	No
Antena 3	antena3internacional.com	NEWS	HTTP+DNS	No	No	No	No	No
Aporrea	www.aporrea.org	NEWS	HTTP	No	No	No	No	No
Armando info	armando.info	NEWS	HTTP+DNS	DNS	DNS	DNS	No	DNS
Caraota digital	caraotadigital.news	NEWS	HTTP+DNS	DNS	DNS	DNS	DNS	DNS
Caraota digital	caraotadigital.xyz	NEWS	HTTP+DNS	DNS	DNS	DNS	DNS	DNS
Caraota digital	www.adncaraota.com	NEWS	HTTP	No	No	No	No	No
Caraota digital	www.caraotadigital.net	NEWS	HTTP+DNS	DNS	DNS	DNS	DNS	DNS
Chronicle One	cronica.uno	NEWS	HTTP+DNS	DNS	DNS	DNS	DNS	DNS
La region newspaper	diariolaregion.net	NEWS	HTTP+DNS	DNS	No	DNS	DNS	DNS
Parallel Dollar	dolarparalelo.biz	NEWS	HTTP+DNS	No	DNS	No	DNS	No
Parallel Dollar	dolarparalelovenezuela.com	NEWS	HTTP+DNS	No	DNS	No	DNS	No
Parallel Dollar	dollarparalelovenezuela.com	NEWS	HTTP+DNS	DNS	DNS	No	DNS	DNS
Dolar today	bit.ly	NEWS	No	HTTP	No	No	No	No
Dolar today	dolartoday.com	NEWS	HTTP	DNS	DNS	DNS	DNS	DNS
Dolar today	dolartoday.info	NEWS	HTTP+DNS	DNS	DNS	DNS	DNS	DNS

SITE	DOMAIN	CATEGORY	CANTV	Movistar	Digitel	Inter	NetUno	Super Cable
Dolar today	dolartoday.org	NEWS	HTTP+DNS	DNS	DNS	DNS	DNS	DNS
Dollar.nu	dollar.nu	NEWS	HTTP+DNS	DNS	DNS	DNS	DNS	DNS
Cocuyo effect	efectococuyo.com	NEWS	HTTP+DNS	DNS	DNS	DNS	DNS	DNS
The newspaper	eldiario.com	NEWS	HTTP	No	No	No	No	No
The Venezuelan Liberal	liberal-venezolano.blogspot.com	NEWS	HTTP+DNS	DNS	DNS	DNS	DNS	DNS
El Nacional	www.el-nacional.com	NEWS	HTTP+DNS	DNS	DNS	DNS	DNS	DNS
El Nacional	www.elnacional.com	NEWS	HTTP+DNS	DNS	DNS	DNS	DNS	DNS
El Pitazo	elpitazo.com	NEWS	HTTP+DNS	DNS	DNS	No	DNS	DNS
El Pitazo	elpitazo.info	NEWS	HTTP+DNS	DNS	DNS	No	DNS	DNS
El Pitazo	elpitazo.net	NEWS	HTTP+DNS	DNS	DNS	DNS	DNS	DNS
The weather	www.eltiempo.com	NEWS	HTTP+DNS	DNS	DNS	DNS	DNS	DNS
eldolarparalelo.info	eldolarparalelo.info	NEWS	HTTP+DNS	DNS	DNS	DNS	DNS	DNS
EVTV	evtv.online	NEWS	HTTP+DNS	DNS	DNS	DNS	DNS	DNS
EVTV	evtvmiami.com	NEWS	HTTP	DNS	DNS	DNS	DNS	No
Infobae	infob.ae	NEWS	HTTP	DNS	DNS	HTTP	DNS	No
Infobae	www.infobae.com	NEWS	HTTP+DNS	DNS	DNS	DNS	DNS	DNS
Infobae	www.infobae.media	NEWS	HTTP+DNS	DNS	DNS	DNS	DNS	DNS
Insight Crime	es.insightcrime.org	NEWS	HTTP	No	No	No	No	No
Insight Crime	www.insightcrime.org	NEWS	HTTP	No	No	No	No	No
The digital herd	lamananadigital.com	NEWS	HTTP+DNS	No	No	No	No	No
The pin	lapatilla.com	NEWS	HTTP+DNS	DNS	DNS	DNS	DNS	DNS
The pin	www.lapatilla.com	NEWS	HTTP+DNS	DNS	DNS	DNS	DNS	DNS
Matured	maduradas.com	NEWS	HTTP+DNS	DNS	DNS	No	DNS	No
Minute 30	minuto30.com	NEWS	HTTP+DNS	DNS	DNS	DNS	DNS	DNS
We monitor	monitoreamos.com	NEWS	HTTP	DNS	DNS	DNS	DNS	DNS
News Update	noticiaaldia.com	NEWS	HTTP+DNS	DNS	DNS	DNS	DNS	DNS
News Update	noticialdia.com	NEWS	HTTP+DNS	DNS	No	DNS	DNS	DNS

SITE	DOMAIN	CATEGORY	CANTV	Movistar	Digitel	Inter	NetUno	Super Cable
Noticias venezuela	noticiasvenezuela.org	NEWS	HTTP+DNS	DNS	DNS	DNS	DNS	DNS
Digital news	www.noticierodigital.com	NEWS	HTTP+DNS	No	No	No	No	No
NTN 24	www.ntn24.com	NEWS	HTTP+DNS	DNS	DNS	DNS	DNS	DNS
First Report	primerinforme.com	NEWS	HTTP+DNS	DNS	No	DNS	DNS	DNS
Cut-off point	puntodecorte.com	NEWS	HTTP+DNS	DNS	DNS	DNS	DNS	DNS
Runrunes	runrun.es	NEWS	HTTP+DNS	No	No	No	DNS	No
Sumarium	sumarium.es	NEWS	HTTP+DNS	No	No	No	No	No
TV Venezuela	www.tvvenezuela.tv	NEWS	HTTP+DNS	DNS	DNS	DNS	DNS	DNS
Venezuela up to date	venezuelaaldia.com	NEWS	No	DNS	No	DNS	DNS	No
Venezuela up to date	www.venezuelaaldia.com	NEWS	No	DNS	DNS	DNS	DNS	No
Vivo play	vivoplay.net	NEWS	HTTP	DNS	DNS	No	DNS	No
VPITV	vpitv.com	NEWS	HTTP+DNS	No	DNS	DNS	DNS	DNS
VPITV	www.vpitv.com	NEWS	HTTP+DNS	DNS	DNS	DNS	DNS	DNS
Soundcloud	soundcloud.com	MMED	HTTP+DNS	DNS	DNS	No	DNS	DNS
LiveStream	livestream.com	MMED	DNS	No	DNS	DNS	DNS	DNS
Reddit	www.reddit.com	MMED	No	DNS	No	No	No	No
Zello	zello.com	MMED	DNS	HTTP	DNS	No	No	No

2.2 Media and Communications

Table showing blocked news media, social media and media distribution websites, during 2022, as recorded by VE sin Filtro.

2.3 Civil society, activism and human rights

Among the various blockades imposed by the State or by compliant Internet Service Providers, VE sin Filtro has found that in Venezuela the websites of some NGOs have been blocked. Several organizations have been victims of blocks over the years, four websites related to human rights and activism were blocked in 2022.

SITE	DOMAIN	CATEGORY	CANTV	Movistar	Digitel	Inter	NetUno	Super Cable
Mi Convive	miconvive.com	HUMR	HTTP+DNS	DNS	DNS	DNS	DNS	DNS
Acceso a la Justicia	accesoalajusticia.org	HUMR	HTTP	No	No	No	No	No
Change.org	www.change.org	HUMR	HTTP+DNS	DNS	DNS	DNS	DNS	DNS
Justicia, Encuentro y Perdón	www.jepvenezuela.com	HUMR	HTTP	No	No	No	No	No

Tabla que muestra los bloqueos activos de las ONG, durante 2022, según lo registrado por VE sin Filtro.

VE sin Filtro determined that the website www.jepvenezuela.com of the NGO Justicia, Encuentro y Perdón (JEP), was blocked in 2022. This organization monitors and documents human rights violations since 2017, often taking action before national and international bodies to ensure justice, protection, and reparations for victims of those violations. The organization represents victims of killings and detentions between 2014 and 2017. The NGO also reports on acts of torture against political prisoners in Venezuelan detention centers. On June 7, 2022, the organization denounced the arbitrary detention of young people by the Chacao municipal police of Chacao after they participated in a public commemoration of Neomar Lander, a 17-year-old who was among the 163 people killed during the 2017 protest cycle.

According to technical measurements conducted by VE sin Filtro, the organization's website has been blocked for CANTV customers since at least June 6, 2022, initially as an HTTP/HTTPS block and currently six active HTTP blocking events. VE sin Filtro also found that ISP Movistar maintains an HTTP block.

The advocacy platform Change.org continues to be blocked, VE sin Filtro confirmed that it has been blocked by CANTV since February 22, 2019, a few days after several media outlets were blocked for covering an event featuring Juan Guaidó. The event, which was intended to mobilize support and promote humanitarian aid, included a concert with Latin American artists on the border with Colombia.

These blocks prevent citizens from accessing important information and tools for civic participation. For example, Change.org is a platform used worldwide to launch and collect signatures for online petitions that are often directed at politicians. For its part, JEP Venezuela promotes access to justice in the country.

Internet censorship also affects the ability of organizations to carry out their work and achieve their objectives. Therefore, blocking access to the websites of these organizations constitutes a violation of the right to free association and a restriction on freedom of expression.

2.4 Censorship circumvention tools

The Venezuelan government is blocking access to censorship circumvention tools such as VPNs and Tor. These blocks have a significant impact on Venezuelans' ability to access information and interact with content and their communities on the Internet.

Major ISPs in Venezuela, including CANTV, during 2022 and 2023 continued to block the TunnelBear and Psiphon VPN websites. TunnelBear's blocking is more comprehensive, as it not only affects access to the website, but also attempts to prevent the VPN itself from working, without success.

In CANTV the blocking is of DNS type in addition to HTTP/HTTPS simultaneously since 2019. While the other providers have maintained the DNS block active since August 20, 2020.

The blocking of Psiphon only affects the website, but users can still access the application through alternative URLs.

CANTV is also attempting to block Tor, a privacy tool that can be used to circumvent censorship. Blocking Tor, VPN and other tools, if more effective, would have a very serious impact on Venezuelans' ability to access online information that would otherwise be restricted.

SITE	DOMAIN	CATEGORY	CANTV	Movistar	Digitel	Inter	NetUno	Super Cable
Hidemyass	www.hidemyass.com	VPN	No	No	No	No	DNS	No
Psiphon	psiphon.ca	VPN	HTTP+DNS	DNS	No	DNS	DNS	DNS
Tunnelbear	api.tunnelbear.com	VPN	HTTP+DNS	DNS	No	No	DNS	DNS
Tunnelbear	tunnelbear.com	VPN	HTTP+DNS	DNS	No	HTTP+DNS	DNS	DNS
Tunnelbear	tunnelbear.com	VPN	HTTP+DNS	DNS	DNS	DNS	DNS	DNS

Table showing active domain blocking of censorship circumvention tools, during 2022.

Restrictions are often comprehensive, or at least try to be. For example, TunnelBear VPN's homepage is not the only page blocked (https://tunnelbear.com), as attempts were also made to alter the application's functionality by blocking communications with their servers via its API (Application Programing Interface, https://api.tunnelbear.com/). In previous years, this blocking of the TunnelBear API affected the normal use of the VPN in Venezuela, as users were unable to register with the application or log in, even if they were already active users. After disclosure, the TunnelBear team modified its operation, allowing Venezuelan users to once again access a fully functional VPN.

In the case of Tor, although users can continue to use Tor and Tor Browser, our measurements confirm that CANTV is blocking parts of the Tor infrastructure in an insufficient attempt to make it inaccessible.

The blocks came amid increased blocking of websites, including high-profile media outlets such as el-nacional.com and lapatilla.com. CANTV blocked the use of Tor directly and used many of the alternative access points available, which are known as bridges. Specifically, it targeted bridges that were pre-installed on Tor.

2.5 Additional blockages from January to October 2023

The website eldiario.com was the first blocked domain of 2023, the blocking started on January 25 at the state-owned CANTV via simultaneous HTTPS and DNS blocks.

On April 26, Salario Digno VZLA, a pivotal website belonging to the Venezuelan Trade Union Network was blocked. This website, among other functions, was an integral part of an organizing effort to collect signatures for a list of demands addressed to the government. It played an important role in advocating for fair wages and improved working conditions, which are pressing issues in Venezuela's current socio-economic landscape. This block coincided with a period of heightened labor unrest, as documented by the Venezuelan Observatory of Social Conflict (OVCS). In the first half of 2023 alone, OVCS recorded 3,754 protests demanding Economic, Social, Cultural, and Environmental Rights, accounting for 86% of all demonstrations in that period. The block of Salario Digno VZLA was implemented across several Internet Service Providers: CANTV, Digitel, and Inter utilized a DNS block, while Movistar opted for a less typical approach of HTTPS/HTTP block, deviating from its usual practice of DNS blocking.

Similarly, the page of the Observatorio de Finanzas has been facing an internet block since May 3, enforced by major ISPs including CANTV, Movistar, Digitel, Supercable, and Inter. This block censors an independent source of information and analysis regarding inflation and economic activity in Venezuela, especially critical in the absence of official data. The country was undergoing a period of social unrest linked to wages and labor demands, making the availability of such information even more vital. Movistar's method of blocking was notably comprehensive, employing both HTTPS/HTTP and DNS blocks, while the other providers implemented DNS blocking.

This pattern of internet censorship in Venezuela, as exemplified by the blocking of Salario Digno VZLA and the Observatorio de Finanzas, sheds light on a broader governmental strategy aimed at suppressing online organizing and information dissemination. The Venezuelan government's actions indicate a concerted effort to quell any form of digital mobilization or collective action that could pose a challenge to its authority.

By targeting these platforms, the government not only stifles voices advocating for social justice and economic reform but also demonstrates an acute sensitivity to any online content perceived as politically sensitive. This approach extends beyond traditional news media to encompass civil society groups, reflecting a comprehensive attempt to control the

digital narrative and limit public access to alternative viewpoints and independent analyses. In a landscape where official data and government narratives often dominate, such acts of censorship significantly hinder the citizenry's ability to stay informed and engage in informed discourse, ultimately leading to the further closing of civic space in Venezuela.

Several news websites were also blocked from January to October of 2023 adding to the already pervasive censorship of independent news sources in the country. **Noticias.com was blocked in all the main ISPs analyzed. The domains focoinformativo.com and opinionynoticias.com are blocked only in Movistar;** in the first domain the blocking is HTTPS/HTTP+DNS type and HTTPS/HTTP type in the second case. These blocks are implemented directly for domains ending in informativo.com and noticias.com respectively, so the page noticias.com also has active HTTPS/HTTP+DNS blocking by Movistar and also DNS blocking by CANTV, Digitel Inter and NetUno.

SITE	DOMAIN	CATEGORY	CANTV	Movistar	Digitel	Inter	NetUno	Super Cable
El Diario	eldiario.com	NEWS	HTTPS+DNS	No	No	No	No	No
Salario Digno Vzla	salariodignovzla.com	HUMR	DNS	HTTPS/HTTP	DNS	DNS	No	No
Finance Observatory	observatoriodefinanzas.com	HUMR	DNS	HTTPS/ HTTP+DNS	DNS	DNS	No	DNS
Informative Focus	focoinformativo.com	NEWS	No	HTTPS/ HTTP+DNS	No	No	No	No
Opinion and News	www.opinionynoticias.com	NEWS	No	HTTPS/HTTP	No	No	No	No
World News	noticias.com	NEWS	DNS	HTTPS/ HTTP+DNS	DNS	DNS	DNS	DNS

Table showing page blocks initiated in the first half of 2023, as recorded by VE sin Filtro.

2.6 Blocks during the opposition primary

VE sin Filtro documented blockades against the infrastructure set up by the National Primary Commission, mainly against the polling place search engine sites and the Commission's web page. In the past, we have documented blocks and other forms of interference using digital technology, aimed at impeding the participation and expression of dissident voices. These practices attack civic space and deny the right to free association.

As of September 7, more than one month before the elections to be held on October 22, a DNS type block was found to be active in Digitel, Inter, Supercable and the state-owned CANTV. Movistar applied a HTTPS/HTTP type blocking.

Later, two domains created for the same purpose were also blocked and since October 14, the same restrictions were applied to the Commission's main website.

SITE	DOMAIN	CATEGORY	CANTV	Movistar	Digitel	Inter	NetUno	Super Cable
Primary search engine 2023	buscadorprimaria2023.com	POLR	DNS	HTTPS/HTTP	DNS	DNS	DNS	DNS
Primary search engine 2023	d1zjwmfds04x7i.cloudfront.net	POLR	DNS	DNS	DNS	DNS	No	No
Primary search engine 2023	d3lokqj5h9z9zs.cloudfront.net	POLR	DNS	DNS	DNS	No	No	No
Primary commissions	comisiondeprimariave.org	POLR	DNS	DNS	DNS	No	No	No
The Venezuela of the encounter	lavenezueladelencuentro.com	POLR	DNS	DNS	DNS	No	No	No

Table listing the blocked domains related to the first days of October 2023, as documented by VE sin Filtro.

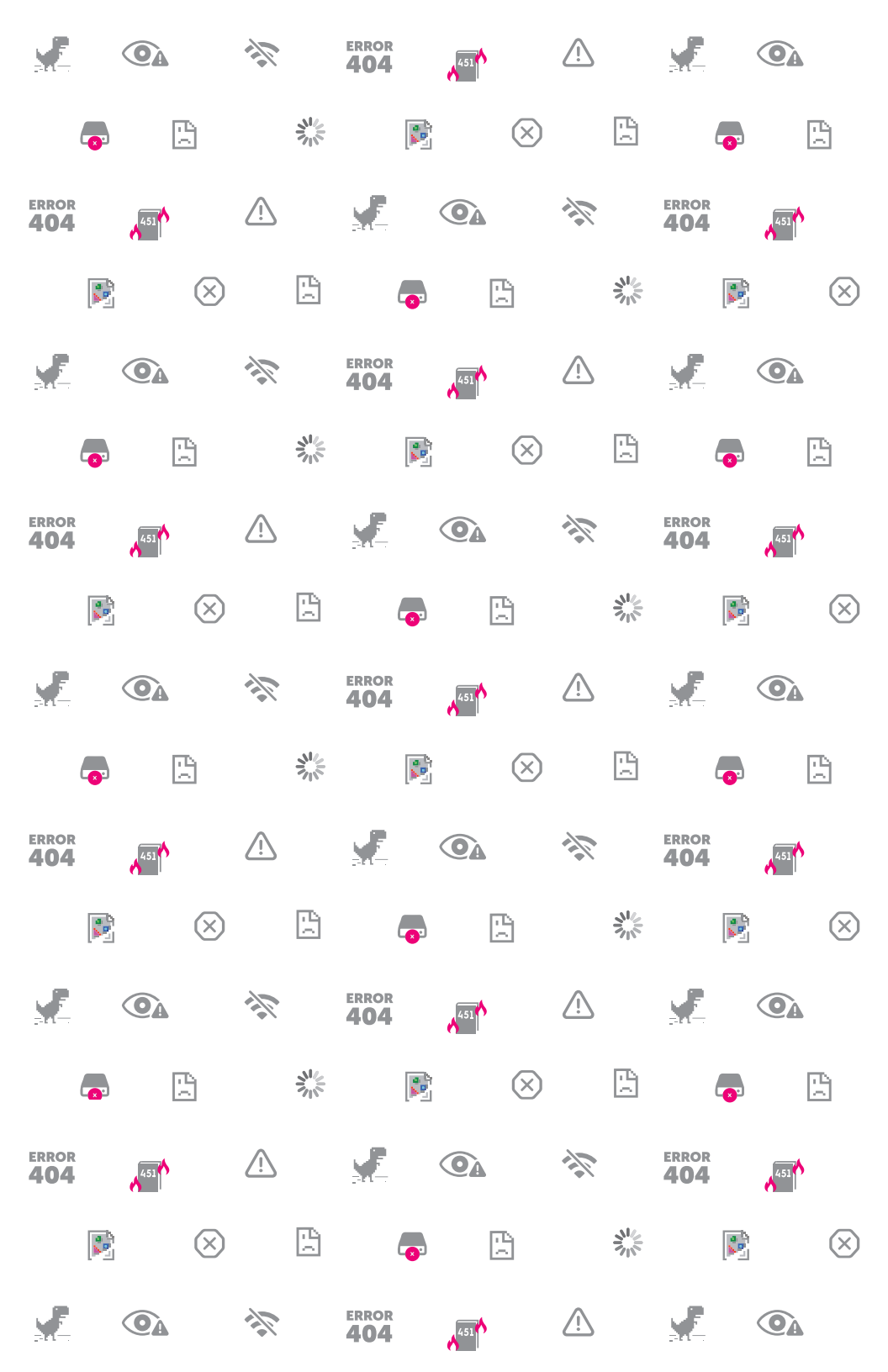
Independently, VE sin Filtro could not confirm the blocking of the results transmission servers, as denounced by the National Primary Commission, however, there are similar antecedents such as the blocking of CANTV to servers of the Voatz application, one of the channels of participation in the 2020 Popular Consultation.

The use of Internet censorship to restrict citizen participation in an event of this nature is a severe attack on civil and political rights, freedom of participation, freedom of association and the rights to elect and be elected.

Including blocks to sites related to the opposition primary election, from January to October 2023 117 domains were blocked, including 16 domains related to political criticism and opposition movements, an increase of 45% over the domains that were blocked in 2022.

CATEGORY	ABBREVIATION	CASES OF BLOCKED WEBSITES	BLOCKED URLS OR DOMAINS	TOTAL BLOCKING EVENTS
E-commerce	COMM	1	4	23
Economics	ECON	2	4	22
Hate Speech	HATE	2	2	9
Human Rights Issues	HUMR	5	6	26
Media Sharing	MMED	3	3	13
News Media	NEWS	48	73	342
Political Criticism	POLR	14	16	70
Pornography	PORN	2	2	2
Public Health	PUBH	2	2	8
Anonymization and circumvention tools	VPN	3	5	26
TOTAL JANUARY-OCTOBER 2023		80	117	541

Table with the number of blocked websites, blocked urls or domains and blocking events by category recorded from January to October 2023.


ERROR
404
451

3 CONNECTIVITY AND AVAILABILITY OF INTERNET SERVICE

Internet connectivity in Venezuela can be described as intermittent. Connectivity outages and interruptions occur regularly, leaving large swaths of the country without connection. As a result, the availability of Internet service has been a problem for many users. The country's economic and political dynamics have negatively affected the development and maintenance of the telecommunications infrastructure and electricity system, on which almost all connections in the country depend. This has resulted in limited and unreliable Internet services over the years.

VE sin Filtro monitors connectivity levels across the country, reporting outages and other large-scale disruptions to Internet connectivity. Outages, or more generally incidents where Internet connectivity drops, can be due to technical problems at an ISP or broader infrastructure issues, such as a power outage, and are visible through ISP- or state-level connectivity metrics.

Incident:
Connectivity failure at national level.

Events:
Reflection of the drop in national connectivity in states or ISPs in particular.

Incidents are classified according to their level of severity (critical, severe or minor) and their origin, such as an outage, ISP failure, or intentional Internet outages. Sometimes the origin cannot be identified. These Internet service interruptions are perceived by users, who often report service interruptions lasting hours and/or days.

When an incident affects several states or ISPs, we consider them as independent "events" that form a single incident. However, this analysis does not include prolonged service failures lasting weeks, months or years.

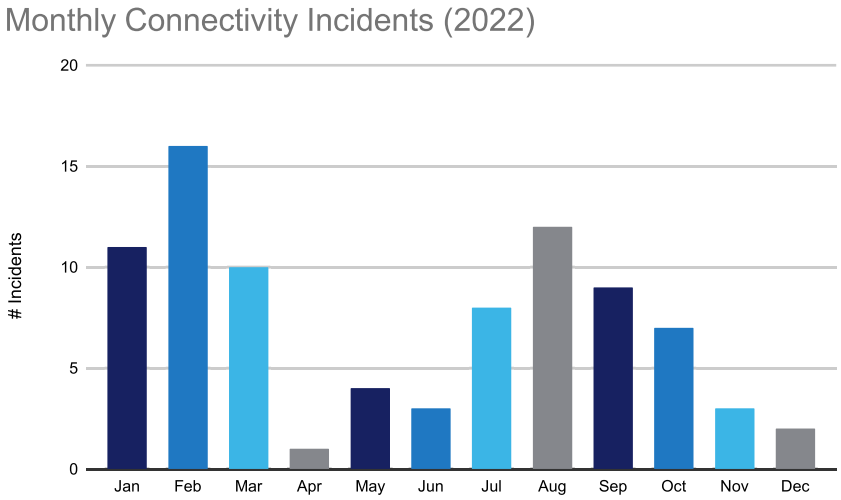
The Internet providers monitored in greater detail by VE sin Filtro are: CANTV, Digitel, Movistar, Intercable, Net Uno and Supercable, as previously mentioned these providers have the highest percentage of market share, according to CONATEL[8][9][10][11].

[8] Conatel. Telecommunications SECTOR FIGURES REPORT I QUARTER 2022
[9] Conatel. Telecommunications SECTOR FIGURES REPORT II QUARTER 2022
[10] Conatel. Telecommunications SECTOR FIGURES REPORT III QUARTER 2022
[11] Conatel. Telecommunications SECTOR FIGURES REPORT IV QUARTER 2022

3.1 Connectivity Incidents

In 2022, VE sin Filtro recorded a total of 86 Internet connectivity interruptions, which is evidence of an 83% increase in the number of incidents recorded during 2021. In both years, the month with the highest number of cases was February, with a total of 16 incidents in 2022. In February 2022, 8 of the incidents originated from ISP NetUno, which reported multiple outages between February 12 and 17. Four of the incidents were due to power outages and the cause of the others is unknown.

In August 2022 there were 12 incidents, of which 5 were caused by outages and 2 by service interruptions at the ISP level. The cause of the other 4 incidents is unknown.

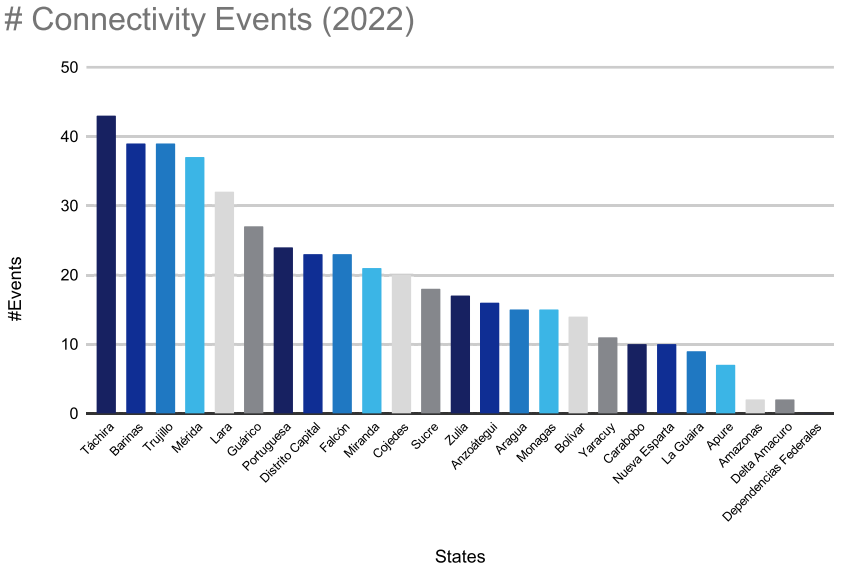


Bar chart showing the number of connectivity incidents on a monthly basis from 2022.

In 2022 there were 474 regional events. Táchira was the most impacted state, with 43 events, followed by 39 events in the states of Barinas and Trujillo, and 37 in Mérida.

OSVP's August 2022 bulletin[12] reveals that San Cristóbal and Mérida had the highest percentage of users reporting daily Internet service interruptions, with 61% and 52.8%, respectively.

[12] https://www.observatoriovsp.org/wp-content/uploads/boletin-38_agosto-2022_primera-entrega-comprimido.pdf



Bar chart showing the number of connectivity incidents by state from 2022.

Events according to the magnitude of the incident

Drops in connectivity levels compared to normal are described according to their magnitude. This work has been categorized by VE sin Filtro:

- **Critical:** 0-50% of connectivity
- **Serious:** 51-80% of connectivity
- **Slight:** A drop that doesnt reach 80% connectivity but coincides with a clear event of decreased connectivity in several states.

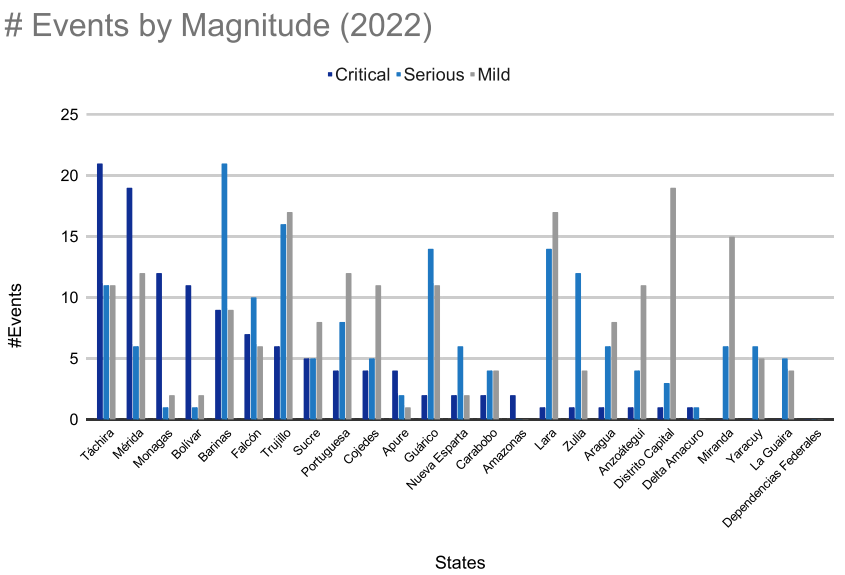
In 2022, Táchira and Mérida had the highest number of critical events (21 and 19, respectively). They were followed by Monagas (12), Bolívar (11) and Barinas (9). In 2021, Táchira and Mérida also had the highest number of critical events. Barinas had the highest number of serious events in 2022 with a total of 21, followed by Trujillo with 16 serious events, and then Guárico and Lara with 14 serious events in both states. Regarding mild events in Distrito Capital there were 19 events in 2022, followed by Trujillo and Lara both with 17 events, Miranda had a total of 15 mild events, finally Portuguesa and Mérida both had a total of 12 events each.

Given that the mostly rural states of Amazonas, Apure and Delta Amacuro and the Federal Dependencies have the lowest penetration rates, detecting and measuring Internet connectivity drops is more difficult than in other states.

Most of the events were mild with a total of 191, followed by severe events with 167 events and critical events with a total of 116 events nationwide.

STATES	CRITIC	SERIOUS	SLIGHT	# EVENTS 2022
Táchira	21	11	11	43
Trujillo	19	6	12	37
Barinas	12	1	2	15
Mérida	11	1	2	14
Lara	9	21	9	39
Distrito Capital	7	10	6	23
Falcón	6	16	17	39
Portuguesa	5	5	8	18
Cojedes	4	8	12	24
Guárico	4	5	11	20
Zulia	4	2	1	7
Sucre	2	14	11	27
Miranda	2	6	2	10
Monagas	2	4	4	10
Anzoátegui	2	0	0	2
Bolívar	1	14	17	32
Nueva Esparta	1	12	4	17
Carabobo	1	6	8	15
Aragua	1	4	11	16
La Guaira	1	3	19	23
Yaracuy	1	1	0	2
Apure	0	6	15	21
Delta Amacuro	0	6	5	11
Amazonas	0	5	4	9
Dependencias Federales	0	0	0	0

Table showing the number of connectivity disruption incidents by state and severity level for 2022.



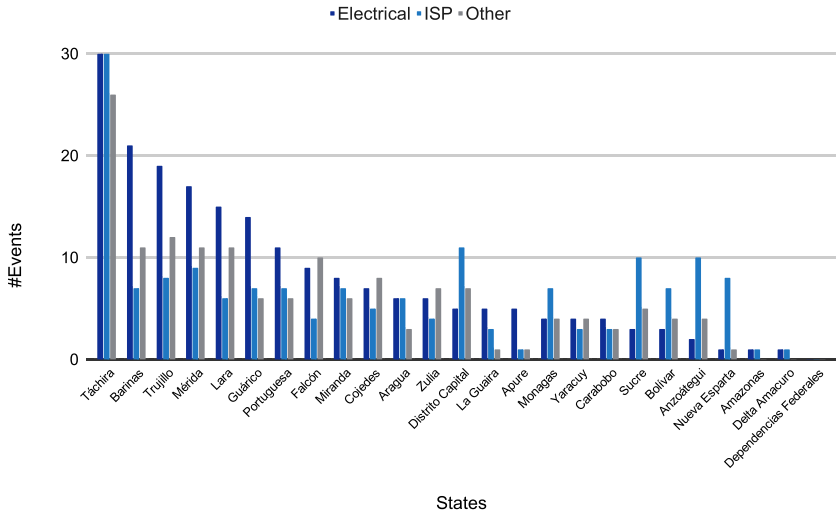
Bar chart showing the number of connectivity events by type (power outage, ISP originated or other) of outage by Venezuelan state or district for 2022.

3.2 Incidents by cause

As for the origin of the incidents, VE sin Filtro identified blackouts or brownouts; ISP-caused failures, mostly due to damaged backbone fiber optic cables or undefined service problems; and "other causes", which are incidents of unknown origin.

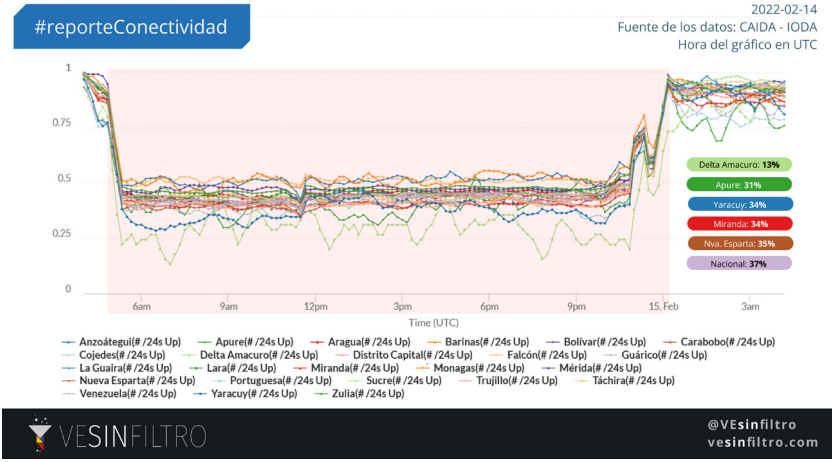
Incidents of connectivity interruption due to power outages decreased in 2022 compared to 2021. With respect to the total number of events recorded, 34.88% were due to power outages, i.e. 201 events. The most affected states are Táchira, Trujillo, Barinas, Mérida, Portuguesa and Lara. Táchira, Mérida and Trujillo have appeared on these lists every year.

Number of Connectivity Events by Outage Type (2022)



Bar chart showing the number of connectivity events by type (power outage, ISP originated or other) of outage by Venezuelan state or district 2022.

On February 14, 2022, there was a nationwide blackout that lasted almost an entire day. It caused a connectivity outage in 23 states for 19 hours and 20 minutes. The incident began at 12:50 a.m. The lowest connectivity level recorded nationwide was 37% compared to normal levels, which qualifies as a critical drop in connectivity. Another 23 incidents had connectivity levels between 0 and 50 percent of normal levels.



Line graph shared on social networks showing the drop in connectivity in most Venezuelan states on February 14, 2022. The connectivity signal is the number of IP /24 segments accessible by active polling, normalized (Source: VE sin Filtro, with data obtained from IODA API).

In relation to incidents identified due to operator or service provider failures, in 2022 there was an increase with respect to the total number of incidents due to ISP failure in 2021.

In 2022, 34.88% of the incidents were of this type, i.e. 30 in total. The state of Táchira was again the most affected, with 30 events in this case, i.e. all incidents of this type affected the state of Táchira.

Incidents due to other causes or of unknown origin accounted for 30.23% of the total. This amounted to 26 incidents. In 2021 only 11 incidents of this type were recorded and Táchira had the highest number of events with a total of 26.

3.3 Incidents and events by duration

Nationwide incidents in 2022 lasted a total of ten days, twelve hours and fifty minutes (for all regional connectivity interruptions recorded). The states with the longest total connectivity failure times were Táchira (eight days, one hour and thirty minutes), Trujillo (seven days, twenty-one hours and ten minutes) and Barinas (seven days, sixteen hours and twenty minutes). The other states were affected within a range of 7 days to 3 hours.

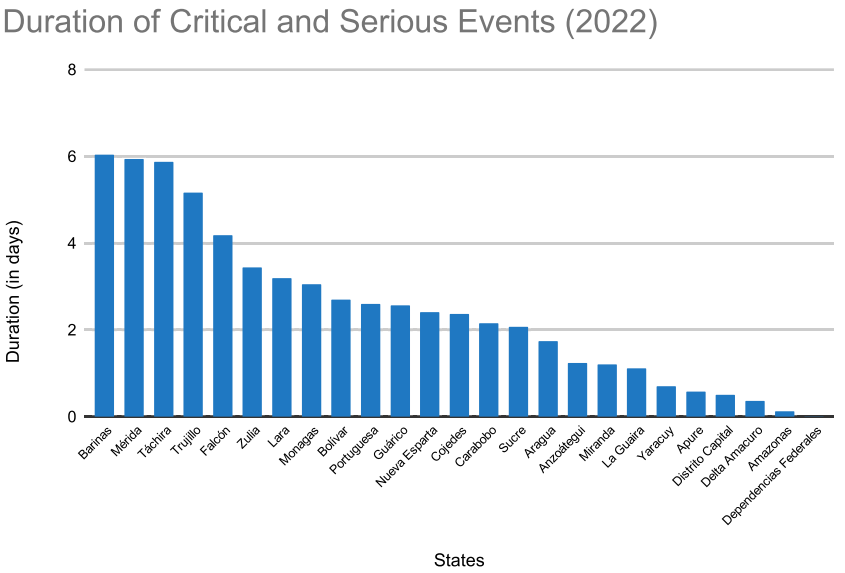
DURATION OF CONNECTIVITY EVENTS (2022)			
STATES	DURATION (DAYS)	AVERAGE (DAYS)	MAX (DAYS)
Táchira	8.06	0.20	0.88
Trujillo	7.88	0.19	0.88
Barinas	7.68	0.20	0.88
Mérida	7.57	0.16	0.88
Lara	6.43	0.20	0.88
Distrito Capital	5.56	0.24	0.88
Falcón	5.26	0.23	0.88
Portuguesa	4.71	0.19	0.54
Cojedes	4.40	0.22	0.88
Guárico	4.22	0.16	0.88
Zulia	4.20	0.25	0.88
Sucre	3.51	0.19	0.88
Miranda	3.45	0.22	0.54
Monagas	3.35	0.27	0.88
Anzoátegui	3.31	0.21	0.54
Bolívar	3.05	0.22	0.54
Nueva Esparta	2.71	0.20	0.88
Carabobo	2.59	0.26	0.88
Aragua	2.58	0.17	0.88
La Guaira	1.69	0.20	0.88
Yaracuy	1.47	0.13	0.44
Apure	0.83	0.12	0.25
Delta Amacuro	0.37	0.18	0.25
Amazonas	0.13	0.06	0.12
Dependencias Federales	0	N/A	N/A
NATIONAL	**10.53**	**0.23**	**0.88**

Table showing the duration of 2022 connectivity events by state, including total DURATION, AVERAGE duration, and LONGEST duration.

Táchira, a border state, was again the most affected in 2022, as reflected by the total duration of the events.

3.4 Duration of Critical and Serious Incidents

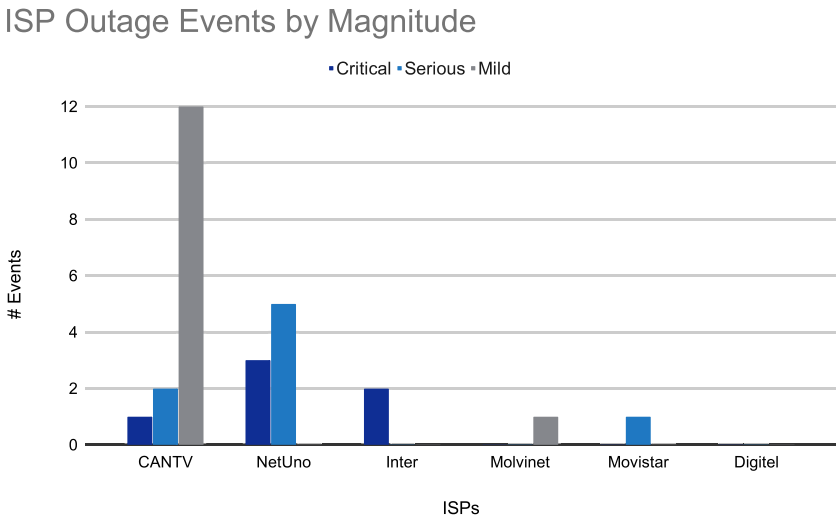
An analysis of the duration of critical and serious incidents shows that Barinas (6 days 59 minutes 2 seconds) is the state with a total of 30 critical and serious events, Mérida with 25 total events with a total duration of 5 days 22 hours 30 minutes, followed by Táchira with 5 days but a total of 32 critical and serious events, are the states with the highest total duration. The rest of the states are in a range of duration between 5 days and 3 hours.



Bar chart showing the duration (in days) of connectivity events by state, critical and serious magnitude, 2022.

3.5 Incidents by ISP failure and by magnitude

The total duration of events due to ISP failures showed that the most impacted were the state-owned CANTV and the private provider NetUno. Connectivity drops due to CANTV outages, confirmed by the provider, accounted for a total of 15 events in 2022. They lasted one day and seven hours in 2021 and three days and thirteen hours in 2022.



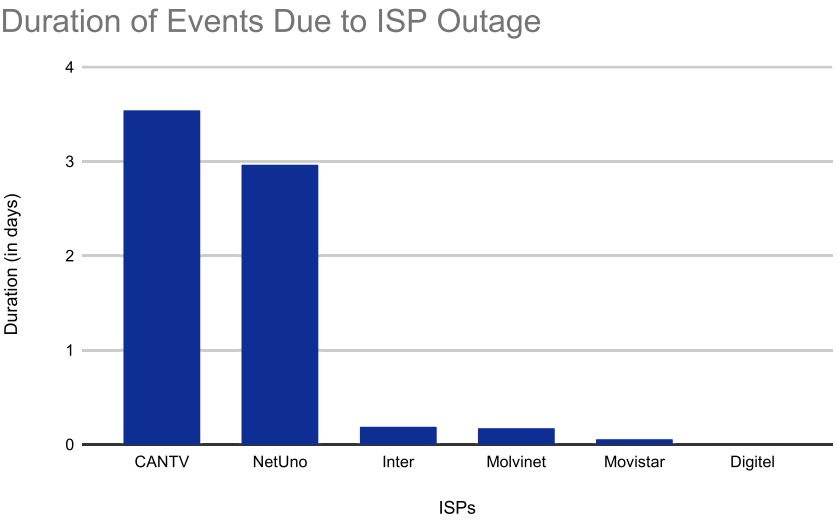
Bar chart showing the number of events due to ISP failures by 2022 provider.

The annual report 2022 of the Humanitarian Social Observatory on Community Monitoring of Public Services pointed out that the country's main Internet provider can only guarantee that less than 5 percent of those who use it do not experience outages. It is important to consider that CANTV in the last quarter of 2022 had more than half (55.92 %) of the Internet market subscribers, according to CONATEL. With respect to NetUno, there was an increase in total outage time to two days, twenty-three hours and ten minutes in 2022. This is due to the 8 connectivity events that took place in February 2022, with a total duration of 5 days. These represent all connectivity down events that affected NetUno in 2022. According to the OVSP, NetUno serves 2.9% of the Venezuelan Internet market.

Line graph shared on social networks showing the drop in NetUno connectivity during February 12-18, 2022. This connectivity signal is the number of IP /24 segments accessible via active polling, normalized (Source: VE sin Filtro, with data obtained from the IODA API).

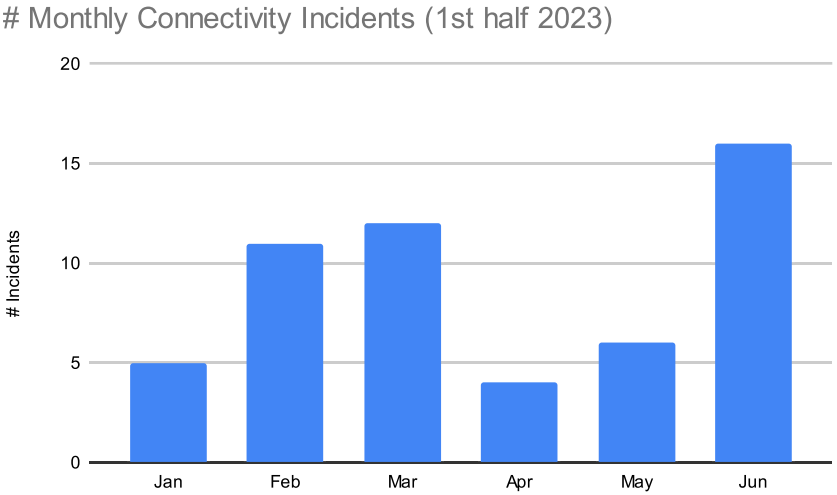
3.6 Failure duration per ISP

Adding up the duration of incidents due to ISP failure, we find that the national state-owned CANTV has a total of 3 days and 13 hours, followed by NetUno with 2 days, 23 hours and 10 minutes, in third place is Inter with 4 hours and 30 minutes, followed by Movilnet with 4 hours and 10 minutes and finally Movistar with 1 hour and 20 minutes of duration, while Digitel and SúperCable do not present any event due to their own failure.



Bar chart showing the duration, in days, of ISP failure events by 2022 provider.

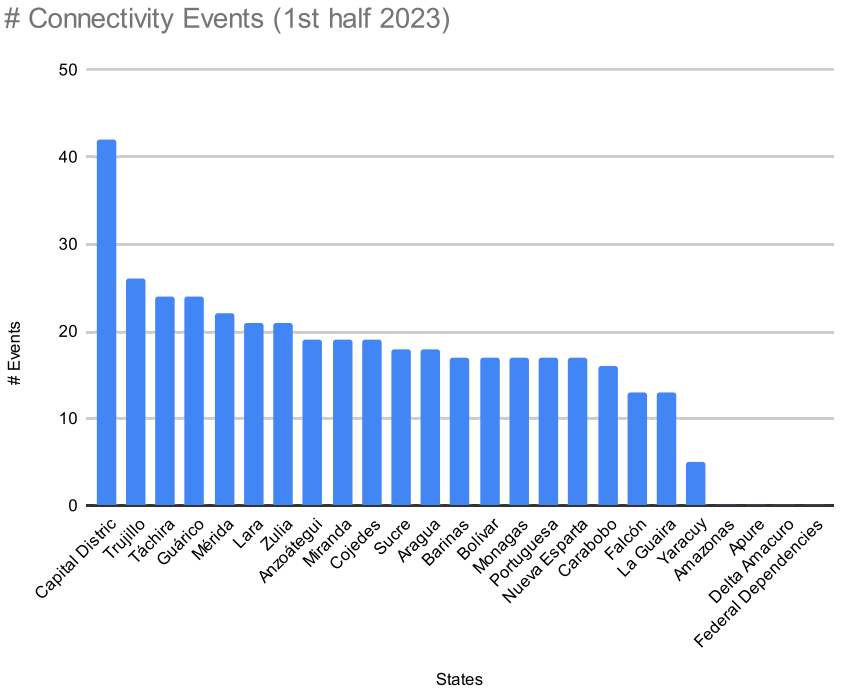
3.7 Incidents in the first half of 2023



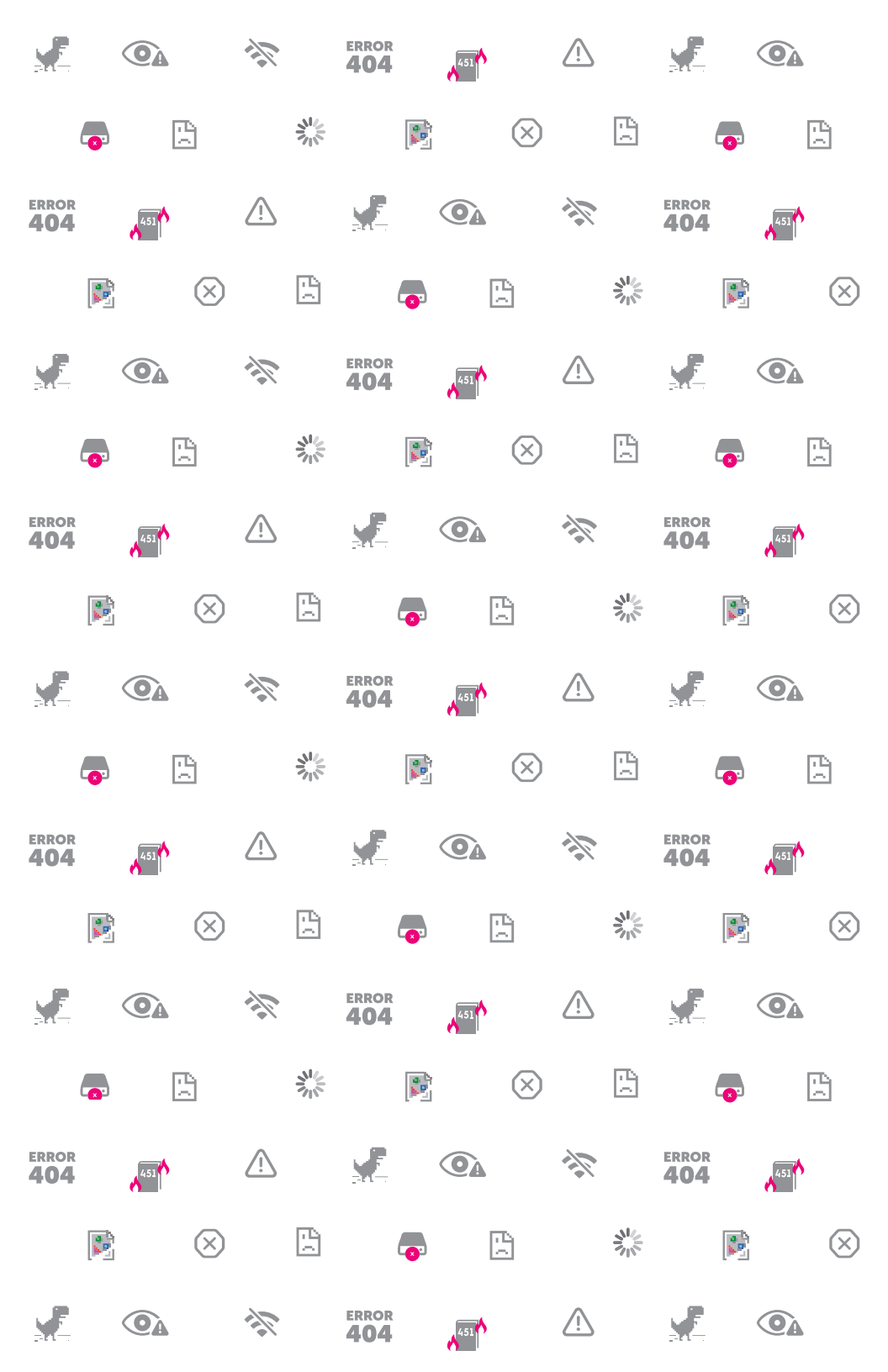
Bar chart showing the number of connectiv ity incidents monthly for the first half of 2023.

For the first half of 2023 VE sin Filtro recorded 54 incidents of connectivity drops, compared to the total number of incidents in 2022. This represents 62.79% of the total incidents that occurred during 2022. June 2023 saw

the highest number of incidents with a total of 16, then followed by March with 12 incidents. These 54 incidents are in turn 405 regional events, 42 of which affected the Distrito Capital. Then among the most affected states are the Andean states of Trujillo, Táchira and Mérida with 26, 24 and 22 regional connectivity downtime events respectively. The state of Guárico is also one of the most affected states with 24 events as well as the state of Táchira.



Bar chart showing the number of connectivity incidents by state for the first half of 2023.


ERROR
404
451

4 PROTECTION OF PERSONAL DATA AND SECURITY OF GOVERNMENT WEBSITES

The protection of personal data is fundamental to the security and privacy of users and citizens. As more and more activities become digitized, the protection of personal data becomes increasingly important.

The ability of individuals to own and control their data is enshrined in international human rights law, including the Universal Declaration of Human Rights and the International Covenant on Civil and Political Rights. The right to privacy includes the protection of personal data. The data itself should be treated as property and individuals should receive fair compensation for it[13].

Everything a person does leaves digital traces that can reveal intimate details of their thoughts, beliefs, movements, associations and activities[14]. Human rights courts have also recognized that almost every step in the handling of personal data (from initial collection to use, retention, and sharing) can interfere with privacy. This means that such actions must be limited to a legitimate aim[15].

Governments and organizations must guarantee and prioritize the protection of individuals' personal data, which must be collected and processed in a transparent, consensual and lawful manner, so that people's rights to privacy and data protection are respected, thus avoiding harming individuals or violating their rights. Individuals should be informed of what data is collected, why it is collected and with whom it is shared. Individuals must also be given the opportunity to consent to the collection and processing of their data.

> In Venezuela there is no specific legislation on privacy or data protection, however, there are isolated provisions in some laws in force that regulate certain aspects related to data protection, in an woefully insufficient manner.

In the absence of tools to ensure the protection of personal data, in the absence of a legal framework and rules to protect them, and in the face of a careless attitude on the part of public entities and private companies to

[13] https://www.economist.com/open-future/2019/01/21/we-need-to-own-our-data-as-a-human-right-and-be-compensated-for-it
[14] https://www.hrw.org/news/2018/04/19/data-privacy-human-right
[15] https://www.weforum.org/agenda/2021/05/data-rights-privacy-human-rights/

make responsible use of data, each citizen needs to take protecting sensitive information into their own hands as much as possible.

Despite any efforts, Venezuelans continue to be highly vulnerable to their data being exposed, used for unexpected purposes, sold, or accessed by third parties. Current laws and regulations fail in providing mechanisms for data protection. They do not prevent data from being collected, used, or transferred to third parties without consent. Nor do they hold organizations, public or private, accountable for data breaches.

In a notable example of such a data breach in July 2023, Banco de Venezuela, the largest bank in the country, suffered a ransomware attack by the criminal gang Lockbit. This incident was reported by VE sin Filtro, based on a post on the gang's website and threat intelligence channels. Despite the severity of the cyberattack, it was initially denied by the bank, which is state-owned. Eventually, after apparently opting not to pay the ransom, a significant amount of data from the bank's servers was published by Lockbit.

We could not find any efforts by the bank to notify or remediate the victims whose personal data was exposed in the breach. The focus of the exposed data was primarily on internal documents and some corporate clients. Had the breach included a wider range of client data, the number of affected individuals could have been much greater. This incident underscores the vulnerability of digital systems and the urgent need for robust cybersecurity measures and transparent reporting protocols in the event of data breaches.

4.1 Security and trust of government websites

It is the responsibility of public and private entities that receive sensitive information from individuals to ensure the security of that information. Their servers must be secure and data must not be accessible to third parties; ensure that users' passwords can be kept secure; establish recovery protocols that are not vulnerable to abuse; and take measures so that users of their systems can know that they are on a genuine site, especially in a context where many users access government sites from public wifi connections, connections managed by third parties or other people's computers.

One of the minimum practices expected of Internet portal operators is that their websites have a TLS/SSL certificate and operate under the HTTPS protocol.

HTTPS
Provides encryption for data transmitted between a user's browser and a website, preventing third parties from intercepting and accessing sensitive information such as passwords and payment method data. This protection is especially important for websites that handle sensitive data, such as the sites of public entities where identity, habitat, labor, tax declaration, among other data provided when carrying out public procedures, are handled.

SSL/TLS certificates

Verify the identity of the website and guarantee that the data transmitted between the user and the website is encrypted and secure, which helps to mitigate the risks and threats associated with cyber-attacks and ensure the peace of mind of its users, such as: man in the middle attacks, being the target of phishing, manipulation of transmitted data, among others.

Two-factor authentication

Is a security method that allows you to confirm your identity when logging in, since passwords are vulnerable to cyber-attacks, this method makes accessing your accounts easier. Is more secure because in order to log in, in addition to the password, you must enter a credential, which can be something you know, something you have, or something you are.

VE sin Filtro analyzed 279 domains of websites belonging to public entities, with .ve domain extension, of which at least 70% of the sites are not served by HTTPS with SSL/TLS certificate signed by a certifying authority recognized by the main web browsers, i.e. the information transmitted and received by these pages is sent and received without and the authenticity of the server cannot be verified.

From this list, 32 sites manage sensitive information, of which 30 have a login, 17 in which you can only have an account if you are previously authorized by the administrator of the site. The remaining 13 sites are pages with login for public use to carry out fundamental procedures such as the Saime page (siic.saime.gob.ve) which allows you to apply for your identity card and passport. Half of them (6 of these) do not have SSL certificates, which means that their information is not encrypted.

Regarding the two-step authentication, only one has the option to activate it, which is the domain to log in to the petro app (petroapp.petro.gob.ve). Of the total of 32 domains there are 2 that are pages for consultation of sensitive data in which it is not necessary to enter your unique and private credentials, such as the CNE page (www.cne.gob.ve), where you can consult significant amounts of data for any voter by entering the national ID number, which is commonly used for mundane transactions, without captcha or rate limits; and the page of the Venezuelan Institute of Social Security (www.ivss.gov.ve), where the data of the citizens are consulted with their ID number and date of birth.

DOMAIN	PUBLIC ENTITY	SSL	2FA
petroapp.petro.gob.ve	Petroapp	TRUE	TRUE
bdvenlinea.banvenez.com	BDVenlínea	TRUE	FALSE
persona.patria.org.ve/login/clave	Patria Purse	TRUE	FALSE
siic.saime.gob.ve	SAIME - Procedures	TRUE	FALSE
tramites.saren.gob.ve	ONLINE PROCEDURES SAREN	TRUE	FALSE
vicesocial.info	Vicesocial Venezuela. Consultation by Cédula UPDATED 2023	TRUE	FALSE
emprenderjuntos.gob.ve/autenticacion	Undertaking Together	TRUE	FALSE
www.cne.gob.ve	National Electoral Council	FALSE	N/A
www.ivss.gov.ve	IVSS Instituto Venezolano de los Seguros Sociales (Venezuelan Social Security Institute)	FALSE	N/A
certificacioninternacional.mijp.gob.ve	Criminal Record Certification	FALSE	FALSE
contribuyente.seniat.gob.ve/iseniatlogin/contribuyente.do	SENIAT - Integrated Customs and Tax Administration Service	FALSE	FALSE
legalizacionve.mppre.gob.ve	Electronic Legalization and Apostille System	FALSE	FALSE
put.intt.gob.ve/login.php	Single Form for Procedures - INTT	FALSE	FALSE
webpi.sapi.gob.ve/indexo.php	WEBPI - Intellectual Property Online System	FALSE	FALSE
www.imprentanacional.gob.ve/certificado_gaceta/site/	Gazette Certification System	FALSE	FALSE
defensa-asegurado.sudeaseg.gob.ve	Insured's Rights and Defense System	TRUE	LOGIN PRIV
fuerzalaboral.sudeaseg.gob.ve/ServidorFL/Proyectos/FuerzaLaboral/index.php	Labor Force	TRUE	LOGIN PRIV
gsr.sudeaseg.gob.ve/login	SIS GSR	TRUE	LOGIN PRIV
rton.sudeaseg.gob.ve/DPCLC_2/Proyectos/DPCLC_2/index.php	sudeaseg	TRUE	LOGIN PRIV
sefam.sudeaseg.gob.ve/Servidor/Proyectos/EstadosFinancieros/index.php	SEFA System of Analytical Financial Statements SEFA	TRUE	LOGIN PRIV
tvl.sudeaseg.gob.ve/login	SUDEASEG |External Users	TRUE	LOGIN PRIV
uam.edu.ve	Arturo Michelena University	TRUE	LOGIN PRIV
virtual.uvm.edu.ve	Momboy Valley University	TRUE	LOGIN PRIV
www.inscripciones.uc.edu.ve	University of Carabobo - DICES	TRUE	LOGIN PRIV
aulavirtual.ujap.edu.ve	Acropolis Platform / José Antonio Páez University	FALSE	LOGIN PRIV
dgpatrimonios.seniat.gob.ve/auth	SENIAT	FALSE	LOGIN PRIV
elegibilidad.banavih.gob.ve	BANAVIH	FALSE	LOGIN PRIV

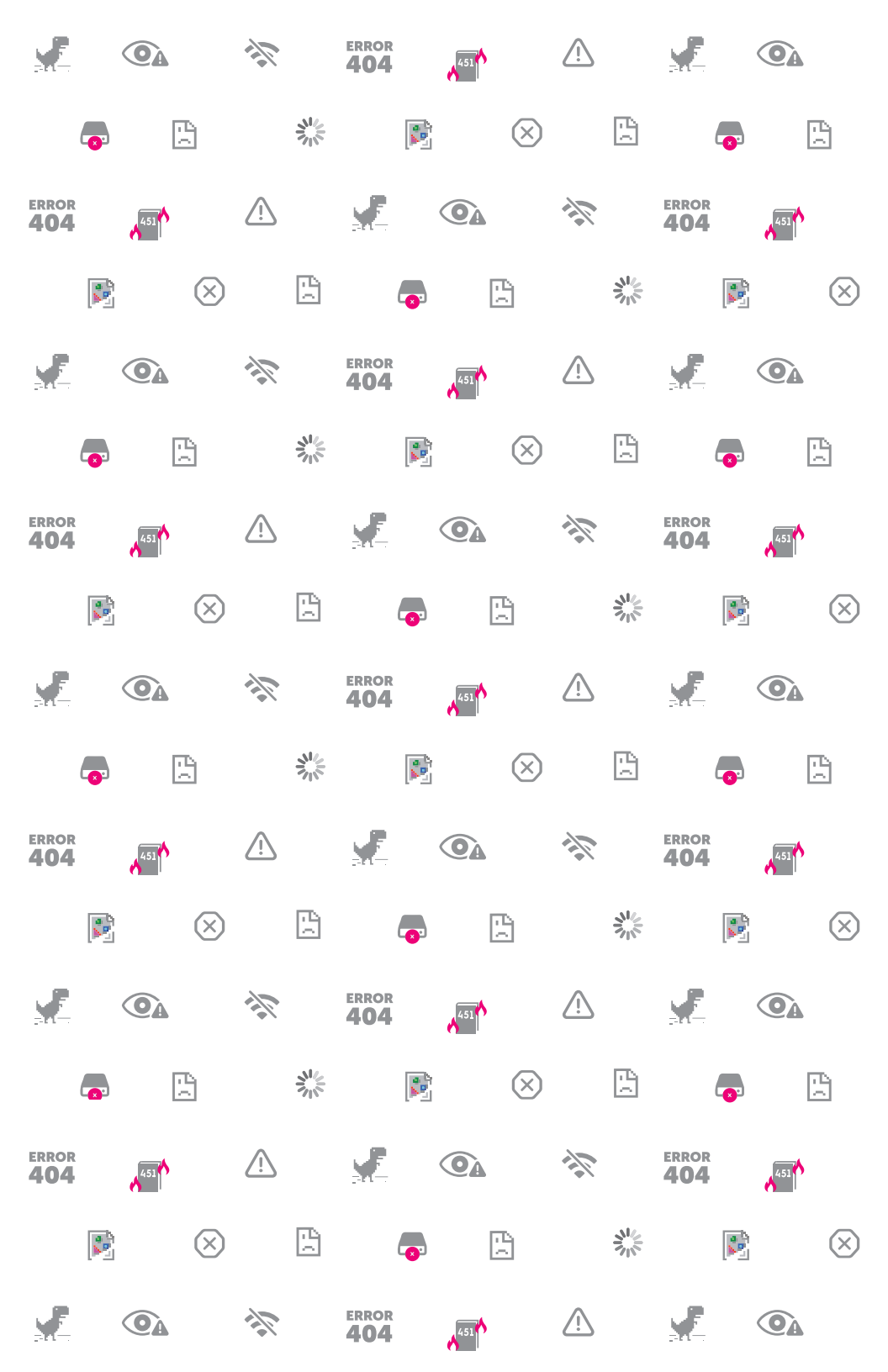
DOMAIN	PUBLIC ENTITY	SSL	2FA
faovel.banavih.gob.ve	FAOV	FALSE	LOGIN PRIV
https://almccs.gob.ve/site/login.html	ALMACENADORA CARACAS	FALSE	LOGIN PRIV
rncenlinea.snc.gob.ve	RNC System	FALSE	LOGIN PRIV
www.tsj.gob.ve	Supreme Court of Justice	FALSE	LOGIN PRIV

Table listing a selection of government websites classified by the availability of SSL/TLS certificates and multiple factor authentication (MFA). MFA can't be verified on websites with only private login.

Another important security factor is the password recovery or change process. The Seniat website, which contains all the tax information of taxpayers, has a recovery option before logging in, which is "Forgot all your information" in which you are asked a mix of easy to guess questions, public and easily accessible personal details to fully reset the account access.

Vulnerable login or password recovery methods on government websites can expose people to many forms of abuse, including identity theft and malicious activities designed to harm users' ability to apply for government assistance, make obtaining government services difficult, and even leave them without valid passports in a country where it can take several months to obtain one.

A significant number of government websites, thankfully fewer than in years prior, do offer an SSL/TLS certificate. However, unlike most genuine websites where the certificate is signed by a trusted third-party authority, confirming the server's authenticity, these government websites often use "self-signed" certificates. This causes the web browser to display a warning that it cannot verify their authenticity. Unfortunately, this has led users to learn to ignore the warning and proceed, which, under normal circumstances, is risky behavior.


ERROR
404
451

5 LACK OF ACCESSIBILITY AS A BARRIER TO EXERCISING RIGHTS ON THE INTERNET

It is impossible to deny the importance of the Internet for full participation in society and the exercise of human rights. However, people with disabilities are seriously unprotected because there are many official portals and information sources that do not meet minimum standards of usability and accessibility.

Although for many the web and the Internet in general is understood primarily as a visual medium, and their interaction with these visual elements occurs with our hands and fingers, the Internet goes much further. Even if a sighted person reads the words on a web page, a blind person could, for example, use software to read the content of the page; a deaf person could watch a video on the Internet and read its subtitles; or a person with a motor disability could ask his or her computer where to click on the screen verbally.

> **When a website or system is poorly designed and implemented, it creates difficulties that make the systems more difficult to use for all types of users, especially those with disabilities.**

The web and the Internet in general is used by countless people with disabilities around the world, but this is made possible by well-designed websites, applications and systems that follow accessibility practices. It is the responsibility of the state to ensure that access to important information and services on the Internet, especially that of the state, are accessible and usable.

The expansion of access to smartphones has helped to make some assistive technologies more common in Venezuela, allowing access to technologies and tools designed for people with disabilities included in the operating system of these devices as well as applications downloaded for this purpose. However, access to smartphones implies a cost bar for some people, some people require different or additional adaptations to those available in mass consumer devices. The effectiveness of these technologies depends to a large extent on the good design of websites, content and applications taking into account best accessibility practices for use with or without the use of these assistive technologies.

Reports from the Venezuelan Confederation of the Deaf (CONSORVEN) show that access to information on the Internet is limited by content that

is not accessible, such as informative videos without subtitles or sign language interpretation. Other examples of content that is not accessible are images that are important for understanding a document or publication without a text description or an informative infographic without an equivalent text.

On the other hand, the vast majority of Venezuelan government web pages, and especially the portals required for essential government procedures such as applying for identity documents, paying taxes, among many others, do not follow basic usability and accessibility practices, making it difficult for some people to use them and possibly making it impossible to manipulate them privately and independently from other people.

The website of the Administrative Service of Identification, Migration and Foreigners, for example, publishes instructions on how to use the page for different procedures with audio videos without subtitles or sign language interpretation, and the page cannot be navigated using the keyboard.

The SENIAT page, on the other hand, is impossible to use with a screen reader since it uses images instead of text, both for section headings and for hyperlinks and buttons necessary to operate the page. The images and hyperlinks are not labeled, have no description or title, making it impossible to operate with a screen reader.

The page of the National Council for Persons with Disabilities (Conapdis), which has accessibility features that are lacking in other government sites, lacks text descriptions of the images that are part of the content, to be used by screen readers.

6 DIGITAL ATTACKS

6.1 Phishing and account theft

In the past it has been identified how the Venezuelan state has used phishing against journalists, dissidents and activists, using everything from highly targeted attacks to several highly sophisticated mass campaigns that manipulated the Internet traffic of an entire provider and is estimated to have affected tens of thousands of victims.

In 2019 and 2020, VE sin Filtro exposed two major state-organized phishing campaigns, one directly targeting Venezuelan dissidents and activists[16] and the other targeting users of a support platform on COVID led by the opposition to Nicolás Maduro.

These attacks employed sophisticated equipment to inspect all traffic from CANTV users, which comprises more than 70% of residential Internet connections, and manipulate Internet traffic to direct them to a fake replica of the website they were trying to visit, even if they correctly typed in the domain name of the genuine page.

Although no new large-scale phishing campaigns such as these have been documented, it is a constant threat. The control over CANTV and the coercive power over private companies, lends itself to phishing attacks and unauthorized access to online service accounts. One of the most common ways is by intercepting the two-step verification SMS or receiving it after acquiring a new SIM for the victim's line.

However phishing on the part of the State is not the only risk**, a trend that began in 2019 but has continued in 2022 and 2023 is the theft of accounts, especially from WhatsApp, the main communication tool used in Venezuela.** Journalists and human rights defenders and citizens in general, have been affected by the theft of WhatsApp accounts.

This account theft mainly occurs for criminal purposes, but it puts at risk sensitive data that is available on the victim's WhatsApp, also allowing the victim's identity to be impersonated. In a politically polarized environment. It is possible that from these phishing attacks criminals will take sensitive information, which appears valuable, to the authorities.

Of particular concern is the possibility that security and intelligence forces are following these same techniques to access the WhatsApp accounts of persecuted individuals, human rights defenders, journalists and activists; but it is difficult to distinguish the origin and motivation of the attack; or that it occurs without any interaction from the victim by intercepting messages or changing SIMs.

[16] https://vesinfiltro.com/noticias/Phishing_by_Venezuelan_government_targets_activists/

6.2 Removal of content from the Internet

The policies of Internet platforms and the responsiveness to third-party requests have an impact on the work for online communication and for the activities of civil society organizations, journalists and the media.

Independent media and civil society organizations in Venezuela are increasingly facing false legal threats and the unfounded abuse of regulatory frameworks for copyright protection in other jurisdictions to provoke the removal of content that is inconvenient to different actors.

In February 2023, El Pitazo denounced that the company Eliminalia, in charge of managing the reputation of politicians, businessmen and even members of criminal groups, uses false copyright claims to force the removal of online content for private clients, and is the same company that has made requests to remove information related to citizens mentioned in articles or investigations about corruption cases.

To achieve its purpose, the firm resorts to different deceptive tactics. One is the sending of petitions to search engines and web hosting companies denouncing false copyright infringement, according to an investigation by the organization Forbidden Stories in its series ¨Story Killers¨.

According to the NGO Freedom House, between May 2019 and March 2021, Eliminalia made at least 16 fraudulent requests to Google on behalf of Venezuelan clients to delete content for copyright infringement under the DMCA (Digital Millennium Copyright Act), a legislation passed in the United States in 1998.

Specially serious cases such as the news website La Gran Aldea (2020) and the non-governmental organization Acceso a la Justicia (2021), which were temporarily taken down, show how DMCA takedown requests affect the exercise of rights. And these tactics, by multiple actors, continued in 2022 and 2023.

6.3 Content review policies and their abuse

The responses of platforms, especially Twitter and YouTube, to sanctions and disinformation coming from accounts associated with the national government have meant that videos and other publications relevant to human rights investigations or referenced in international human rights reports have disappeared.

Some online service providers restrict the use of or access to their services for Venezuelans, in an over-compliance with the sanctions they are obliged to abide by, depending on the jurisdiction from which they operate. Many international financial technology companies have stopped providing services to Venezuelan clients, placing them in an even more vulnerable situation.

Multiple users and independent media have had their social media accounts sanctioned for violating the platforms' rules on fake news and violent images when covering, documenting or commenting on statements

by public officials; not by promoting the desinformation. Many digital platforms distinguish between sensitive or harmful content published by users and publications that denounce or document facts, as in the case of the media, but often independent media in Venezuela end up having difficulties due to content review.

Platforms should proactively publish clearer guidelines designed for journalists and media on how they can document harmful content without violating the rules and what to do if content is unfairly removed.

6.4 Intimidation and threats

The use of social networks and other online platforms to harass journalists, civil society organizations, activists and the media continues. These actions are often especially aggressive against journalists, women and other marginalized communities that share opinions.

The Press and Society Institute of Venezuela (IPYS Venezuela) calls this phenomenon "digital harassment", especially when there are campaigns to discredit and threaten journalists. Although there are no quantitative records of all violations that have occurred to date, researchers have documented examples that show an increase in aggressions in this ecosystem since 2019.

Cases of digital gender-based violence and its impact on women's rights are significant. These aggressions often include attacks with a high sexist content and statements that belittle a person's opinions based on their gender.

As an example, Espacio Público addressed this situation by reviewing three case studies in May 2022. These cases focused on the experiences of Diana Liz Duque, a biologist researching wildlife conservation, and journalists Gregoria Díaz and Lorena Arraiz.

According to IPYS Venezuela, Venezuelan government officials have replicated and amplified the violence that originates in the digital space. The organization published a report on the abuse to which female journalists were subjected that same year, noting that their rights "are mainly violated in social networks". Five journalists were victims of threats, offensive statements and limitations on their privacy.

SOURCE	CATEGORY	NUMBER OF DOCUMENTED INCIDENTS 2022
IPYS Venezuela	Stigmatizing discourse	62
	Attacks and aggressions	55
Public Space	Intimidation	83
	Verbal harassment	44
	Threats	23

Table showing the number of incidents recorded by category in 2022. Hate, discrimination and other forms of abuse that can occur online, according to data recorded by Ipys Venezuela and Espacio Público. Incidents include both those that occurred online and offline (Data source: Ipys Venezuela and Espacio Público).

6.5 Attacks and hacking of servers

Attacks on digital infrastructure, such as web servers, are another common threat against organizations in Venezuela. The most common type of attack is the Denial of Service (DoS) attack against websites of media organizations.

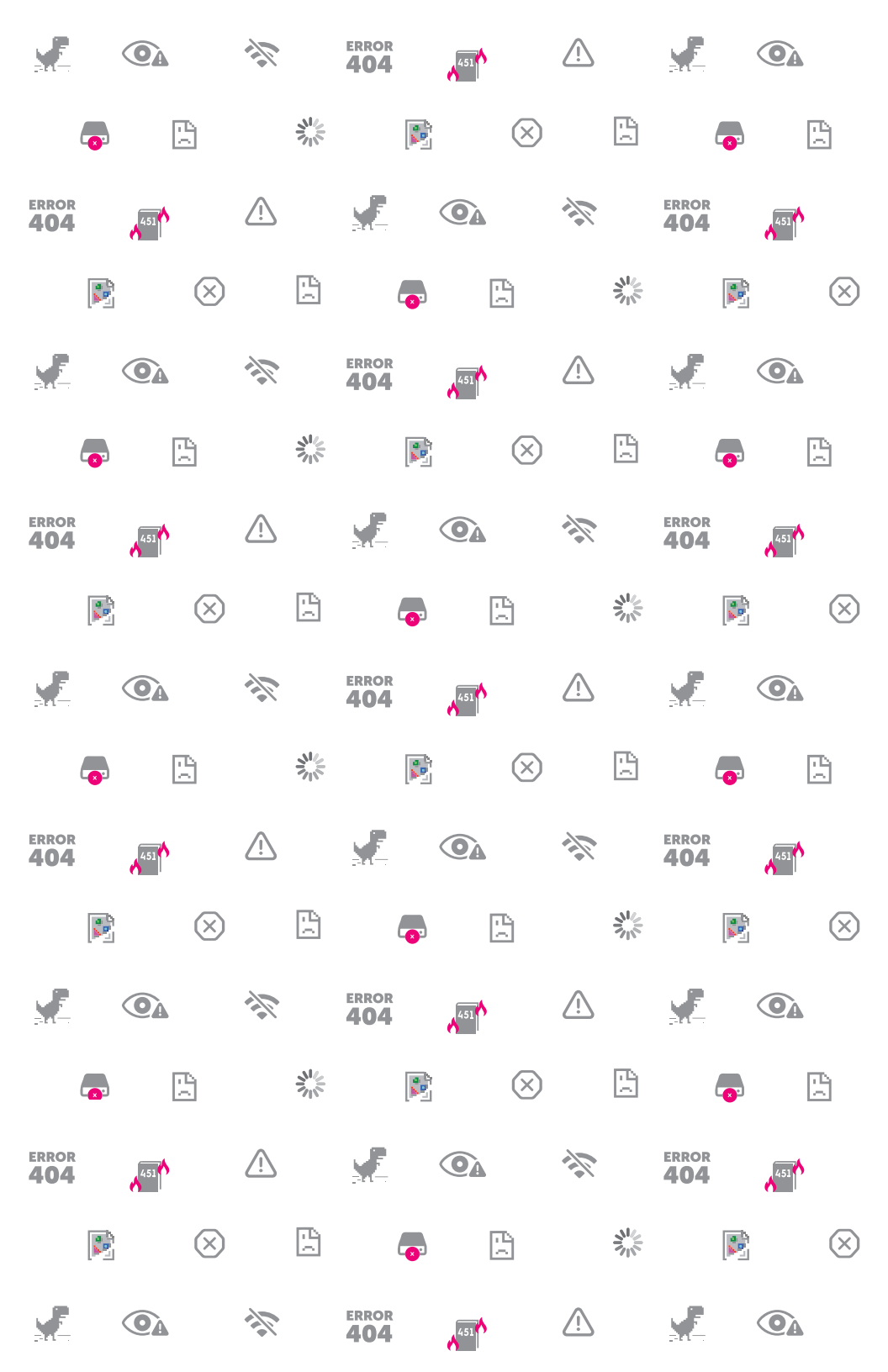
DoS
In a DoS attack, a malicious actor generates an extreme volume of traffic to the target web server until it is unable to respond to legitimate requests from its users due to the overwhelming volume of traffic requests. This type of attack can be carried out in a variety of ways, including attacker-owned devices, using compromised third-party devices or even contracting the service of criminal groups.

DDos
A DoS attack can also become a Distributed Denial of Service (DDoS) attack if the traffic comes from a large number of coordinated devices rather than a few larger sources.

DoS attacks have been reported by many media outlets and usually coincide with a breaking news story that is in the interest of silencing government or related business interests. If the actors behind an attack manage to disable or completely disable a web server while a new or viral news story is in the spotlight, the impact of the report will be reduced.

Some DoS attacks appear to be motivated by economic and business interests, while others are carried out for political reasons, such as when a news story exposes corrupt business practices or is politically hostile to the perpetrator.

Organizations at risk should ensure that their websites and other systems are secure. Some Venezuelan websites have claimed to have been victims of targeted hacks, in which attackers could have gained administrative access to their organization's web servers or data. This is a serious risk; Some of the incidents observed, rather than being targeted hacks, were DoS attacks, ransomware or attacks that automatically find and compromise vulnerable systems. Outdated or misconfigured servers have been a problem, as observed on multiple occasions by VE sin Filtro.


ERROR
404
451

7 THREATS TO PRIVACY

The right to privacy is severely limited in Venezuela in multiple ways, affecting in turn the exercise of other rights, especially the right to freedom of expression. Threats to privacy range from sophisticated computer attacks to the examination of equipment such as cell phones and computers under pressure.

The privacy of communications, the tracking of Venezuelans' social network activity and even the real-time location of people by cell phone are a threat to any citizen, but especially affect journalists, activists, politicians and other civic actors.

Surveillance and monitoring of citizens through technology sometimes works as a large network, massively affecting large numbers of users, and sometimes highly targeted. Occasionally using multiple methods and technologies in the same action.

Despite the policies of major international social media platforms to ignore requests for user information from Venezuelan authorities; the same should not be expected of companies officially operating in Venezuela, nor the growing number of applications managed by the Government, in which it should rather be assumed that authorities can access any information within them, including information that may appear to be private.

7.1 Social media monitoring

According to the Press and Society Institute of Venezuela, one of the mechanisms of persecution against journalists that has been established in recent years is persecution through the use of stigmatizing discourse, criminalization of journalistic work and smear and disinformation campaigns through social networks, among other platforms.

Throughout 2022, this organization totaled 62 violations in the category of stigmatizing speech, which represented 28 incidents of insults or disqualifications of public officials or influential figures, 18 acts of criminalization and 16 systematic smear and disinformation campaigns. Specifically, these events affected 31 journalists and 21 media outlets. https://ipysvenezuela.org/2023/03/05/periodismo-bajo-las-sombras/

For years, civil society organizations have documented reprisals and persecution against citizens for simply making a legitimate use of their freedom of expression on the Internet, from public tweets to the content of their WhatsApp statuses. Surveillance of Venezuelans' online activity, especially on social networks and messaging platforms such as WhatsApp is also supported in part by individuals aligned with the government and channels to report some of these messages.

Although many messages critical of the government are transmitted without much consequence on social networks, the risk of persecution for opinions expressed on the Internet has a silencing effect on certain criticisms by individuals, especially in public spaces for users with openly identified accounts.

An illustrative case is that of Yohn Alejandro Noguera in June 2022, who was arrested[17] by the Bolivarian National Guard (GNB) after he criticized the GNB via WhatsApp. Subsequently, Noguera was charged with "incitement to hatred".

Also in 2022, Venezuelan authorities arrested[18] Olga Mata, a 72-year-old TikTok user, and charged her with hate crimes after she posted a satirical video mocking Nicolás Maduro, his wife Cilia Flores, Cabello and the late Hugo Chávez.

On Sunday, November 13, 2022, the Scientific, Criminal and Criminalistic Investigations Corps (CICPC) reported[19] that it arrested two persons for instigating hatred after they made derogatory comments about the president of the National Racetrack Institute, and well-known member of the ruling party, Antonio Álvarez. The detainees were identified as Denys Jesús Custodio, 34, and Robert José Yañez, 57. Both used Twitter to make comments allegedly "denigrating" Álvarez.

It is now commonplace[20] for government officials to initiate politically motivated cases that result in the arbitrary detention of people for expressing their opinions, as a way of restricting political opposition.

7.2 Surveillance and telecommunications interception

The state apparatus for intercepting Venezuelan's telecommunications is massive, and was revealed in mid-2022 in a transparency report by Telefónica, the parent company of Movistar Venezuela, the most important cell phone operator in the country.

The report indicates that in 2021 Movistar intercepted the communications of 1 million 584 thousand 547 lines of its customers in Venezuela, more than 20% of the telephone or Internet lines, as we presented in a June 2022 publication. These interceptions were allegedly made on orders of the government of Nicolás Maduro in a massive violation of the right to privacy.

The 2022 report omitted all figures on Venezuelan government requests to the company. The opacity in this transparency report could come from government pressures or Telefónica's interest in managing its reputation after the impact of VE sin Filtro's findings contextualizing the 2021 report,

[17] https://espaciopublico.ong/gnb-detuvo-a-ciudadano-por-criticas-en-estados-de-WhatsApp/

[18] https://www.washingtonpost.com/nation/2022/04/19/tiktok-venezuela-arrested-free-speech-censorship-nicolas-maduro/

[19] https://www.radiofeyalegrianoticias.com/detenidas-dos-personas-por-comentar-en-contra-del-potro-alvarez/

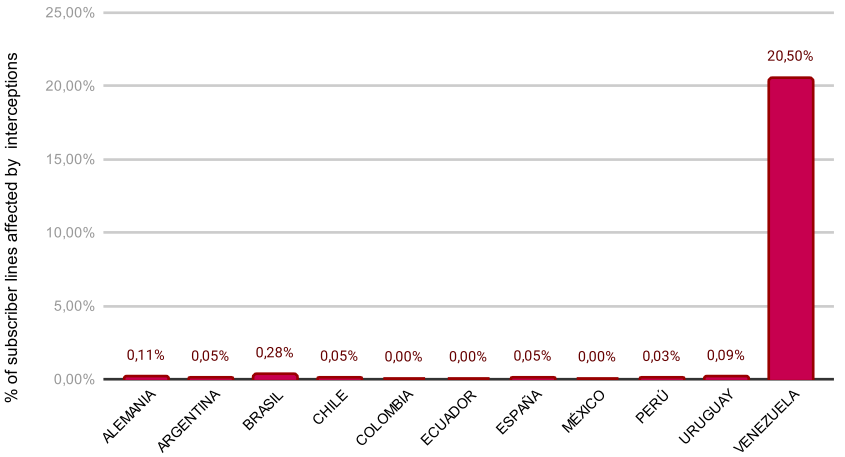
[20] https://cronica.uno/entre-enero-y-noviembre-de-2022-detuvieron-a-13-personas-por-incitacion-al-odio/

which made it into news stories in the Washington Post, El País and reports from the United Nations.

The figures for interceptions by the other telephone and Internet service operators are unknown, as they do not submit transparency reports, but it must be assumed that they are similar, or possibly worse in the case of the state-owned companies. The idea that 20% or more of the telephone lines or Internet connections in other operators may also have been spied on by the government in some way is a highly authoritarian prospect.

In contrast, interception requests by other countries, in the other markets where Movistar operates, do not reach 0.3% of the subscriber lines, in the worst case.

Communication interceptions in 2021, according to Telefonica



Bar chart showing the percentage of customer lines from Telefónica's subsidiary companies affected by telecommunications interceptions in different countries. (Source: VE sin Filtro, using data from Telefónica's transparency reports)

At the same time it could be known:

- Subscriber lines affected by interceptions: 1,584,547 (21% of lines)
- Subscriber lines affected by metadata requests: 997,679 (13% of lines)
- Movistar Venezuela telephone lines and Internet service accesses: 7,730,000
- Rate of Subscriber lines affected by requests of both types: 33%.
- The number of Subscriber lines affected by interceptions increased 7 times from 2016, when it was 234,932 affected accesses
- They do not receive requests for court orders, but from investigative, police, military, intelligence and even the security university UNES.

In addition to the delivery of telecommunications metadata, which in itself is highly sensitive and private, interceptions can include the delivery of the content of phone calls, the content of SMS text messages, the location of individuals by their cell phones or the monitoring of their Internet traffic, without giving detailed figures on each.

For Movistar Venezuela, the competent authorities to request the interception of communications are: the Public Prosecutor's Office, the CICPC, police bodies "empowered to exercise powers in criminal investigation" and strangely the National Experimental University of Security (UNES).

Similarly, the authorities competent to demand metadata about communications and subscriber data (things like: who a user calls, how long calls last, what the subscriber data is, etc) are many of the same, including military and law enforcement agencies.

Nowhere does it mention that the orders come from courts or come with the approval of judges, as they do in other countries, seeming to imply that these are the entities from which they have received these requests, never with the validation of courts.

In the Venezuelan legislation cited by Movistar, interception requests must be approved by a judge to be valid, with particular exceptions such as the case of emergencies and flagrancy, in which the CICPC may make the request, but even in these cases, the Public Prosecutor's Office must be notified and it must be recorded in the case file.

Abuse in the collection of communications metadata is also a violation of people's rights when it is not done in a way that respects human rights. The location of individuals, with whom they communicate, by what means,

for how long and how often, is as sensitive information as the content of those communications.

Furthermore, although no public reports have detailed the use of spyware installed on mobile phones — which would enable the government to spy on the contents of devices, and monitor the communications and activities of their targets— some incidents reported by users suggest its use at some level. It is highly plausible that the Venezuelan government has access to and utilizes such tools. This aligns with their documented use of data extraction tools on devices they physically control. Given the context of widespread human rights abuses and the government's unrestrained surveillance powers, dissidents, investigative journalists, and human rights defenders should regard this as a serious potential threat.

International human rights standards establish that any interception of communications (of any kind) must meet at least these conditions:

- Legitimate objective: It must pursue a legal interest necessary in a democratic society and respectful of human rights, such as investigating a crime.
- Necessary: A practice that could violate rights should not be used if it is not necessary to pursue those legitimate purposes.
- Proportional: As the use of surveillance interferes with human rights, it should be used only when it is proportional to the seriousness of the crime to be investigated, the amount of data obtained should be minimized to only what is necessary, access to this information should be controlled only for approved purposes, and information that is not relevant should be discarded.
- That it is adequately supported by law
- Under a court order from a court of competent jurisdiction independent of the authority concerned with the surveillance of communications
- Allowing due process, notifying the person whenever possible and maintaining transparency of the process

Privacy is a fundamental and inalienable human right, which in turn is key to the free exercise of freedom of expression and association, among other rights.

7.2 Video surveillance

Video surveillance in many Venezuelan cities represents a threat to privacy that is not sufficiently understood and requires further research. Little

or no information is available on the capabilities of the installed systems and their ability to interact with each other.

The Venezuelan government has invested more than US$1 billion in video surveillance and related emergency response projects. Caracas and many other Venezuelan cities have networked video surveillance cameras in strategic locations. Some official figures mention a system of more than 30,000 cameras, known as VEN-911, managed by the government and set up by a consortium of Chinese companies including Huawei, CEIEC and ZTE. These video surveillance systems are likely to monitor, track and record protests or other political activities and possibly help locate and track the movements of individuals of interest to security forces.

The full capabilities of the systems installed in Venezuela are unknown. **There are cameras that record license plates at the entrances and exits of Caracas and possibly other cities, which authorities can use to track the movement of vehicles; and some armored vehicles,** as well as mobile command units of the National Police, include camera systems on an extendable pole.

The same Huawei-CEIEC consortium has sold systems in other countries under contracts that have included facial recognition capabilities, drones for surveillance and data integration with geolocation of targets. A New York Times report revealed that intelligence officials in Ecuador have direct access to transmissions from its equivalent system, ECU-911, despite claims that it is used exclusively for public security[21].

However, this central government system is only one of many sources of video surveillance, as systems apparently managed by municipalities have also been established.

Most notably, in December 2022, the Chacao municipality in Caracas launched a new video surveillance system that included facial recognition capabilities, with no further information related to the use of the videos, capabilities, policies, procedures, who has access to them, and whether they interface with VEN-911. The Chacao municipality did not respond to a public information request from VE sin Filtro regarding the facial recognition capabilities, usage protocols, and possible real-time access by the national government to their video surveillance system.

Chacao police in June 2022 detained a group of political activists and handed them over to the National Police Special Operations Group,[22] suggesting closer cooperation with national security forces in politically sensitive situations than many assumed.

There are other camera systems of a similar kind between public and private spaces, such as near shopping malls and public squares, many of which lack clear ownership, whether private, municipal or otherwise.

[21] https://www.nytimes.com/2019/04/24/technology/ecuador-surveillance-cameras-police-government.html

[22] https://elpitazo.net/politica/pintar-grafitis-la-razon-por-la-que-detuvieron-a-cuatro-jovenes-en-chacao/

7.3 Data extraction, deletion and review of devices under duress

In 2022 and 2023 it is still common for state security forces to demand access to sensitive materials, data and conversations on digital devices, such as cell phones, computers and cameras. Without any regular procedure or authority for this.

It is common for such access to occur during protests or in situations where national government mismanagement is evident. Examples of places or times when such access might take place are: in long lines for services, in deteriorating health care institutions, or during periods of food shortages. These are opportunities where security forces have forced journalists, citizens and activists to allow the content of their devices to be searched, or forced to erase photographic material or recordings, seriously curtailing freedom of expression and information; or simply practicing arbitrary confiscation, not to say theft.

There is under-reporting of such incidents, but press freedom organizations have documented cases against journalists. **Espacio Público documented more than thirty-one cases in thirteen regions of Venezuela between January 2020 and August 2021, mainly targeting journalists, including eighteen instances of illegal seizures of devices and thirteen attempts to search the contents of devices under threat or through the use of violence.** In addition to these risks, organizations such as Venezuela Inteligente have found direct evidence of data extraction from laptops and cell phones of detained journalists who had their devices in the custody of prosecutors and criminal investigators.

At-risk individuals should assume that, in the event of an arrest, any devices in their possession, and possibly devices in their home or office, will be examined and data will be extracted from them at the time of a lawful or unlawful arrest. They should also expect that law enforcement will obtain, through coercive means, any passwords protecting those devices or online services.

Additionally, Venezuelan authorities have acquired Cellebrite UFED Touch units over the years, despite sanctions. These devices are used to hack locked cell phones and extract data from them. Venezuelan authorities, including the General Directorate of Military Counterintelligence (DGCIM), are known to use them.

Surreptitious extraction of data from your digital devices can occur whenever a person loses physical control, even temporarily, to law enforcement custody. This could include when entering secure facilities where devices are not permitted, but also during brief interrogations and other similar scenarios.

More recently we have documented multiple cases of equipment being inspected, during irregular interrogations of at least six members of different civil society organizations, when crossing the air border at international airports, some them were subjected to this multiple times.

During the interrogatories, **the victims were asked about the content of their devices, and they were often coerced into unlock them and answer questions while the officers inspected documents, contacts, communications and other content.**

In the majority of cases, devices with sensitive and personal information were also taken into another room, possibly for data extraction, some of them while unlocked. This worrying trend matches increased persecution against civil society, and civic actors should take precautions.

8 TECHNICAL METHODOLOGY

The documentation of blockages and connectivity incidents is done following the technical methods summarized below.

8.1 Internet blocks

We understand an Internet block as a **deliberate technical measure with the intention of preventing access to an information, services, or servers on the Internet** by interfering with the normal behavior of internet traffic. This occurs intentionally with the purpose of censoring and controlling what citizens can do and see online, through the use of one or more technical measures.

The implementation of web content blocking events can have different motivations.

At VE Sin Filtro we use the following criteria to determine that something the Internet is being blocked:

- It's identifiable
- Measurable
- Consistent
- It is understood how the blockage operates and other explanations for the observed behavior can be ruled out.

Blocking events: blocking events are mainly documented as events, to avoid the ambiguity that can exist when different blocking actions affect the same Internet service. The term “blocking event” refers to the blocking of a URL, domain or IP address, using a specific blocking technique and by a particular ISP.

For example: the URL "caraotadigital.xyz" belonging to the website of the news media Caraota Digital, presents 7 blocking events, 6 DNS type blocks by the ISPs CANTV, Digitel, Movistar, Inter, Net Uno and Supercable, and one HTTP block by CANTV, for a total of 7 blocking events registered in the same case.

Blocking Cases: all blocking events against the same service or website are considered as one case, which groups together blocking events against different domains, as well as each form of censorship implemented by different ISPs.

In order to measure Internet censorship in Venezuela, standardized network measurements were systematically performed and manual network measurements were performed to confirm some results from various ac-

cess points on the network. These are analyzed by VE sin Filtro and compared with other measurements and information sources.

Most of the standardized measurements, are performed with OONI Probe software. The most common measurements include:

- Web Connectivity
- Tor
- Tor Bridge Reachability
- WhatsApp
- Facebook Messenger
- Telegram

OONI's web connectivity test is designed to measure whether websites are being blocked by DNS manipulation, TCP/IP blocking, or whether traffic is being selected for blocking based on details reported in the HTTP or HTTPS protocols. This test is automatically performed both from both a user perspective and an uncensored control perspective.the user's point of view and from an uncensored control point of view. If the results from both perspectivesviewpoints match, the tested website will most likely be accessible. However, if the results differ, the measurement is flagged as anomalous.

To monitor the accessibility of popular instant messaging platforms over time, we conducted OONI's WhatsApp, Facebook Messenger and Telegram tests.

We monitor the accessibility and performance of censorship circumvention tools using a mix of techniques. We manually test the performance of a list of VPNs and other anti-censorship tools manually, we measure access to anti-censorship tool sites using through the OONI web connectivity test, and we also runperform OONI tests for specific tools, especially Tor.

8.2 Connectivity

The technical analysis of connectivity levels, both in real time and after the fact, is mainly performed using proprietary systems that consult data from IODA (Internet Outage Detection and Analysis) and the Georgia Institute of Technology, which generates a history of connectivity data worldwide.

This data, obtained through the IODA API, is processed and analyzed to identify connectivity outages onfailures at a national level, while also conducting and at the same time an investigation is carried out to determine the origin of the connectivity outagefailures. The IODA data is complemented with queries in Cloudflare Radar and Google Traffic Transparency report.

A connectivity outage is defined as an incident that has a different impact, which influences differently in each state of the country, so each regional

outage or disruptionoutage in a particular ISP caused by a specific incident is defined as an event.

In terms ofWith respect to the criteria for identifying incidents/events, two classifications of Internet connectivity loss have been established: were established where Internet connectivity falls:

1. Magnitude of the drop in connectivity levels:
    a. Critical: if it is between 0% and 50%.
    b. Severe: if it is between 50% and 80%.
    c. Minor: if a drop is observed that is not less than 80%, and at the same time coincides with an evident connectivity drop event. It does not refer to normal fluctuations.
2. Cause of incident:
    a. Due to electrical failures
    b. Due to Internet provider failures
    c. Other

The main signal used to assess the severity of these incidents is the connectivity measured by IODA as the active polling of IP addresses from the Internet, counting the number of small segments of IP addresses (/24 network segments) that are considered connected to the Internet if the addresses of the segmentsegment's addresses could be contacted. It is important to know that the measurements have as metric /24 network segments normalized with respect to the highest connectivity value of the region or ISP, which is being monitored.

The main objective of this process is to identify large-scale (macroscopic) connectivity outages that significantly affect the country and/or a region and/or an Internet service provider in Venezuela.

ANNEX

Sites blocked in 2022 and 2023

www.accesoalajusticia.org	Acceso a la Justicia	HUMR	HTTP	No	No	No	No	No	No	No	No	No	No	No
soundcloud.com	SoundCloud	MMED	DNS + HTTP/ HTTPS	DNS	DNS	DNS	DNS	DNS	No	No	DNS	DNS	DNS	DNS
livestream.com	Vimeo Livestream	MMED	DNS	DNS	No	No	DNS	DNS	DNS	DNS	DNS	DNS	DNS	DNS
zello.com	Zello	MMED	DNS	DNS	HTTP	DNS	DNS	DNS	No	No	No	No	No	No
www.reddit.com	Reddit	MMED	No	No	DNS	DNS	No	No	No	No	No	No	No	No
www.2001.com.ve	2001	NEWS	HTTP/HTTPS	DNS	No	No	No	No	No	No	No	No	No	No
6topoder.com	6to poder	NEWS	DNS	DNS	DNS	DNS	DNS	DNS	DNS	DNS	DNS	DNS	DNS	DNS
ww1.6topoder.com	6to poder	NEWS	#N/A	DNS	#N/A	No	#N/A	DNS	#N/A	DNS	#N/A	No	#N/A	No
alnavio.com	Al navio	NEWS	DNS + HTTP/ HTTPS	DNS	DNS	DNS	DNS	DNS	DNS	DNS	DNS	DNS	DNS	DNS
albertonews.com	Alberto News	NEWS	DNS + HTTP/ HTTPS	DNS + HTTPS	DNS	DNS	DNS	DNS	DNS	DNS	DNS	DNS	DNS	DNS
awsveanews.com	Alberto News	NEWS	HTTP	DNS	No	No	No	No	No	No	No	No	No	No
b1tly4n3s.com	Alberto News	NEWS	HTTP	DNS	No	No	No	No	No	No	No	No	No	No
www.b1tlydns02io.com	Alberto News	NEWS	HTTP	HTTPS/DNS + HTTP	No	No	No	No	No	No	No	No	No	No
alekboyd.blogspot.co.uk	Alek boyd	NEWS	DNS	DNS	DNS	DNS	DNS	DNS	No	No	DNS	DNS	DNS	DNS
alekboyd.blogspot.com	Alek boyd	NEWS	No	No	DNS	DNS	DNS	DNS	No	No	DNS	DNS	DNS	No
analisis24.com	analisis 24	NEWS	No	No	DNS	DNS	No	No	DNS	DNS	DNS	DNS	No	No
antena3internacional.com	Antena 3	NEWS	DNS + HTTP	DNS	No	No	No	No	No	No	No	No	No	No
www.aporrea.org	Aporrea	NEWS	HTTP/HTTPS	DNS + HTTPS	No	No	No	No	No	No	No	No	No	No
armando.info	armando info	NEWS	DNS + HTTP/ HTTPS	DNS	DNS	DNS	DNS	DNS	DNS	DNS	No	No	DNS	DNS

DOMINIO	SITIO	CATEGORIA	CANTV		Movistar		Digitel		Inter		Netuno		Supercable	
			2022	2023	2022	2023	2022	2023	2022	2023	2022	2023	2022	2023
airtm.com	Airtm	COMM	#N/A	DNS	#N/A	DNS	#N/A	DNS	#N/A	No	#N/A	DNS	#N/A	DNS
www.airtm.com	Airtm	COMM	DNS + HTTP	DNS	DNS	DNS	DNS	DNS	DNS	DNS	DNS	DNS	DNS	DNS
www.airtm.io	Airtm	COMM	DNS + HTTP	DNS	DNS	DNS	DNS	DNS	DNS	DNS	DNS	DNS	DNS	DNS
www.airtmo.com	Airtm	COMM	DNS + HTTP	DNS	DNS	DNS	DNS	DNS	DNS	DNS	DNS	DNS	DNS	DNS
aguacateverde1.blogspot.com	Aguacate Verde y Dolar Today	ECON	DNS + HTTP	DNS	DNS	DNS	DNS	DNS	No	No	DNS	DNS	DNS	DNS
dolarparalelo.net	Dolar Paralelo	ECON	DNS + HTTP	DNS	DNS	DNS	DNS	DNS	No	No	DNS	DNS	DNS	DNS
dolarparalelo.org	Dolar Paralelo	ECON	DNS + HTTP	DNS + HTTPS	DNS	DNS	DNS	DNS	DNS	DNS	DNS	DNS	DNS	DNS
dolarparalelo.tk	Dolar Paralelo	ECON	DNS + HTTP	DNS	DNS	DNS	DNS	DNS	No	No	DNS	DNS	DNS	DNS
quelacreo.com	que lacreo	HATE	DNS	DNS	DNS	DNS	DNS	DNS	DNS	DNS	DNS	DNS	DNS	DNS
ww12.quelacreo.com	Que lacreo	HATE	#N/A	DNS + HTTPS	#N/A	No	#N/A	No	#N/A	No	#N/A	DNS	#N/A	No
miconvive.com	Caracas Mi Convive	HUMR	DNS	DNS	DNS	DNS	DNS	DNS	DNS	DNS	DNS	DNS	DNS	DNS
miconvive.org	Caracas Mi Convive	HUMR	#N/A	DNS	#N/A	No	#N/A	No	#N/A	No	#N/A	No	#N/A	No
www.change.org	Change.org	HUMR	HTTP	DNS + HTTPS	DNS	DNS	DNS	DNS	DNS	DNS	DNS	DNS	DNS	DNS
www.jepvenezuela.com	JEP Venezuela	HUMR	HTTP/HTTPS	DNS + HTTPS	HTTP/HTTPS	No	No	No	No	No	No	No	No	No
observatoriodefinanzas.com	Observatorio de Finanzas	HUMR	#N/A	DNS	#N/A	HTTPS/DNS + HTTP	#N/A	DNS	#N/A	DNS	#N/A	No	#N/A	DNS
salariodignovzla.com	Salario Digno VZLA	HUMR	#N/A	DNS	#N/A	HTTP/HTTPS	#N/A	DNS	#N/A	DNS	#N/A	No	#N/A	No

www.el-carabobeno.com	El carabobeño	NEWS	No	DNS	No	HTTPS	No	DNS	No	DNS	No	DNS	No	No
eldiario.com	El diario	NEWS	HTTP	DNS + HTTPS	No	No	No	No	No	No	No	No	No	No
www.el-nacional.com	El Nacional	NEWS	HTTP/HTTPS	DNS + HTTPS	DNS	DNS	DNS	DNS	DNS	DNS	DNS	DNS	DNS	DNS
www.elnacional.com	El Nacional	NEWS	DNS	DNS	DNS	DNS	DNS	DNS	DNS	DNS	DNS	DNS	DNS	DNS
elpitazo.info	El Pitazo	NEWS	DNS + HTTP	DNS	DNS	DNS	DNS	DNS	No	No	DNS	DNS	DNS	DNS
elpitazo.com	El Pitazo	NEWS	DNS + HTTP	DNS	DNS	DNS	DNS	DNS	No	No	DNS	DNS	DNS	DNS
elpitazo.net	El Pitazo	NEWS	DNS	DNS	DNS	DNS	DNS	DNS	DNS	DNS	DNS	DNS	DNS	DNS
www.eltiempo.com	El tiempo	NEWS	DNS	DNS	DNS	DNS	DNS	DNS	DNS	DNS	DNS	DNS	DNS	DNS
eldolarparalelo.info	eldolarparalelo.info	NEWS	DNS + HTTP	DNS	DNS	DNS	DNS	DNS	DNS	DNS	DNS	DNS	DNS	DNS
evtv.online	EVTV	NEWS	DNS	DNS	DNS	DNS	DNS	DNS	DNS	DNS	DNS	DNS	DNS	DNS
evtvmiami.com	EVTV	NEWS	HTTP/HTTPS	HTTPS/DNS + HTTP	DNS	DNS	DNS	DNS	DNS	DNS	DNS	DNS	DNS	No
focoinformativo.com	Foco informativo	NEWS	#N/A	No	#N/A	HTTPS/DNS + HTTP	#N/A	No	#N/A	No	#N/A	No	#N/A	No
www.infobae.media	Infobae	NEWS	DNS + HTTP	DNS + HTTPS	DNS	DNS	DNS	DNS	DNS	DNS	DNS	DNS	DNS	DNS
infob.ae	Infobae	NEWS	HTTP	DNS	DNS	DNS	DNS	DNS	HTTP	HTTP	DNS	DNS	No	No
www.infobae.com	Infobae	NEWS	DNS + HTTP/ HTTPS	DNS	DNS	DNS	DNS	DNS	DNS	DNS	DNS	DNS	DNS	DNS
es.insightcrime.org	Insight Crime	NEWS	HTTP	DNS + HTTPS	No	No	No	No	No	No	No	No	No	No
www.insightcrime.org	Insight Crime	NEWS	HTTP	DNS + HTTPS	No	No	No	No	No	No	No	No	No	No
lamananadigital.com	La manada digital	NEWS	DNS + HTTP/ HTTPS	DNS + HTTPS	No	No	No	No	No	No	No	No	No	No
lapatilla.com	La patilla	NEWS	DNS + HTTP	DNS + HTTPS	DNS	DNS	DNS	DNS	DNS	DNS	DNS	DNS	DNS	DNS

DOMINIO	SITIO	CATEGORIA	CANTV		Movistar		Digitel		Inter		Netuno		Supercable	
			2022	2023	2022	2023	2022	2023	2022	2023	2022	2023	2022	2023
caraotadigital.news	Caraota digital	NEWS	DNS + HTTP/ HTTPS	DNS	DNS	DNS	DNS	DNS	DNS	DNS	DNS	DNS	DNS	DNS
caraotadigital.xyz	Caraota digital	NEWS	DNS + HTTP/ HTTPS	DNS + HTTPS	DNS	DNS	DNS	DNS	DNS	DNS	DNS	DNS	DNS	DNS
www.adncaraota.com	Caraota digital	NEWS	HTTP	DNS + HTTPS	No	No	No	No	No	No	No	No	No	No
www.caraotadigital.net	Caraota digital	NEWS	HTTP/HTTPS	DNS + HTTPS	DNS	DNS	DNS	DNS	DNS	DNS	DNS	DNS	DNS	DNS
cronica.uno	cronica.uno	NEWS	DNS	DNS	DNS	DNS	DNS	DNS	DNS	DNS	DNS	DNS	DNS	DNS
diariolaregion.net	Diario La region	NEWS	DNS + HTTP/ HTTPS	DNS + HTTPS	DNS	DNS	No	No	DNS	DNS	DNS	DNS	DNS	DNS
dolarparalelo.biz	Dolar Paralelo	NEWS	DNS + HTTP	DNS	No	No	DNS	DNS	No	No	DNS	DNS	No	No
dolarparalelovenezuela.com	Dolar Paralelo	NEWS	DNS + HTTP	DNS	No	No	DNS	DNS	No	No	DNS	DNS	No	No
dollarparalelovenezuela.com	Dolar Paralelo	NEWS	DNS + HTTP	DNS	DNS	DNS	DNS	DNS	No	No	DNS	DNS	DNS	DNS
ww38.dollarparalelovenezuela.com	Dolar Paralelo	NEWS	#N/A	DNS + HTTPS	#N/A	DNS	#N/A	DNS	#N/A	DNS	#N/A	DNS	#N/A	DNS
bit.ly	dolar today	NEWS	No	No	HTTP	HTTP	No	No	No	No	No	No	No	
dolartoday.com	Dolar today	NEWS	DNS	DNS	DNS	DNS	DNS	DNS	DNS	DNS	DNS	DNS	DNS	DNS
dolartoday.info	Dolar today	NEWS	DNS	DNS	DNS	DNS	DNS	DNS	DNS	DNS	DNS	DNS	DNS	DNS
dolartoday.org	Dolar today	NEWS	DNS	DNS	DNS	DNS	DNS	DNS	DNS	DNS	DNS	DNS	DNS	DNS
dollar.nu	dollar.nu	NEWS	DNS + HTTP	DNS	DNS	DNS	DNS	DNS	DNS	DNS	DNS	DNS	DNS	DNS
efectococuyo.com	Efecto cocuyo	NEWS	DNS	DNS	DNS	DNS	DNS	DNS	DNS	DNS	DNS	DNS	DNS	DNS

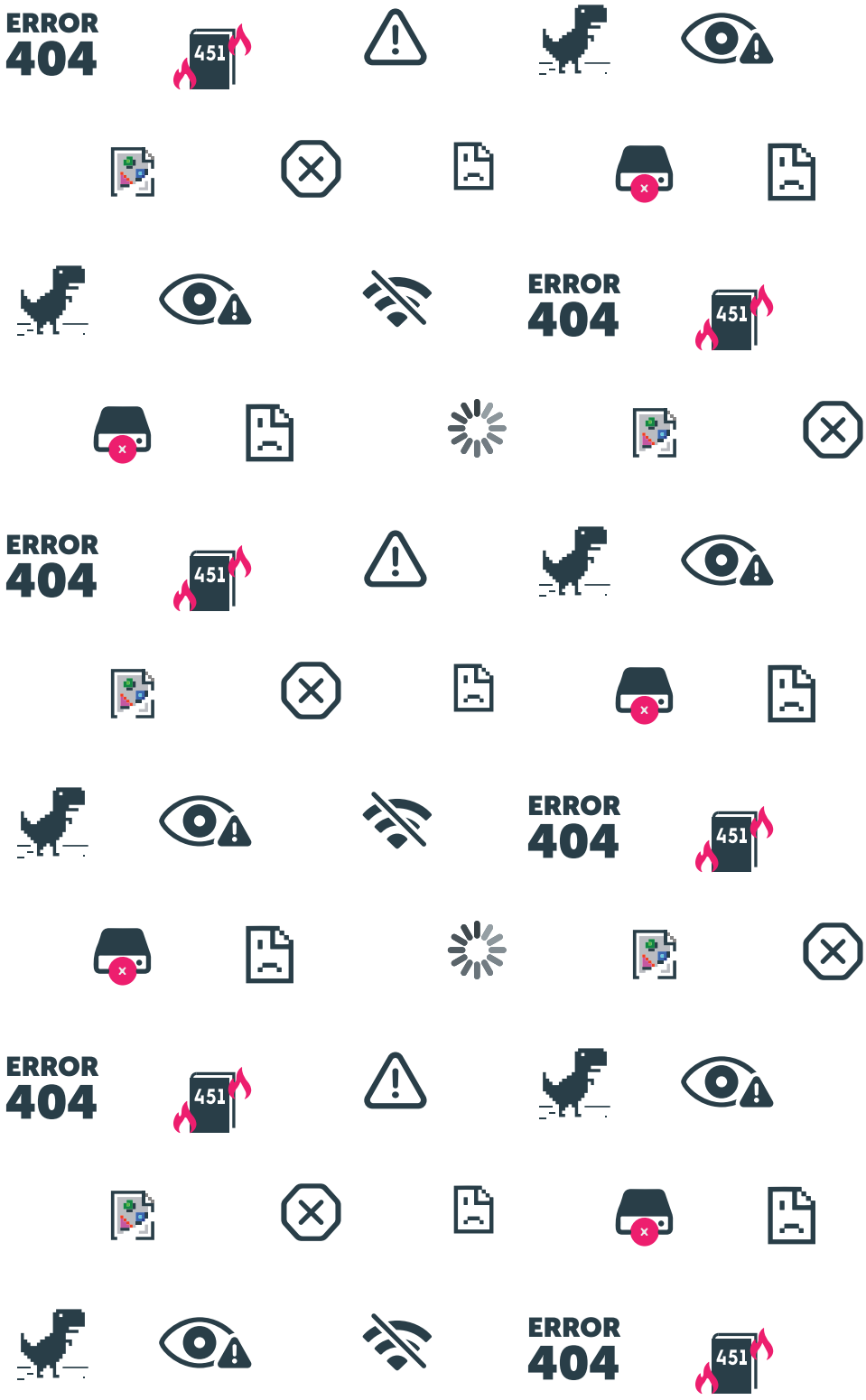
runrun.es	Runrunes	NEWS	DNS	DNS	No	No	No	No	No	No	DNS	DNS	No	No
sumarium.es	Sumarium	NEWS	HTTP/HTTPS	DNS + HTTPS	No	No	No	No	No	No	No	No	No	No
www.tvvenezuela.tv	TV Venezuela	NEWS	DNS	DNS	DNS	DNS	DNS	DNS	DNS	DNS	DNS	DNS	DNS	DNS
venezuelaaldia.com	Venezuela al dia	NEWS	No	No	DNS	DNS	No	No	DNS	DNS	DNS	DNS	No	No
www.venezuelaaldia.com	Venezuela al dia	NEWS	No	No	DNS	DNS	DNS	DNS	DNS	DNS	DNS	DNS	No	DNS
vivoplay.net	Vivo play	NEWS	HTTPS	HTTPS	DNS	DNS	DNS	DNS	DNS	No	DNS	DNS	No	No
vpitv.com	VPITV	NEWS	DNS + HTTP/ HTTPS	DNS + HTTPS	DNS	No	DNS	DNS	DNS	DNS	DNS	DNS	DNS	DNS
www.vpitv.com	VPITV	NEWS	DNS + HTTP	DNS + HTTPS	DNS	DNS	DNS	DNS	DNS	DNS	DNS	DNS	DNS	DNS
www.aguacateverde.com	www.aguacateverde.com	NEWS	DNS + HTTP	DNS	DNS	DNS	DNS	DNS	No	No	DNS	DNS	DNS	DNS
venezuelazonagris.com	Venezuela Zona Gris	NEWS	DNS + HTTP/ HTTPS	#N/A	DNS	#N/A	DNS	#N/A	DNS	#N/A	DNS	#N/A	DNS	#N/A
telesurlibre.com	TeleSur Libre	NEWS	DNS	#N/A	DNS	#N/A	DNS	#N/A	DNS	#N/A	DNS	#N/A	DNS	#N/A
bit.ly/venezuela911	Dolartoday	NEWS	No	#N/A	HTTP	#N/A	No	#N/A	No	#N/A	No	#N/A	No	#N/A
sunoticiero.com	Su Noticiero | Portal de noticias de Venezuela	NEWS	DNS + HTTP/ HTTPS	#N/A	DNS	#N/A	DNS	#N/A	DNS	#N/A	DNS	#N/A	DNS	#N/A
vcrisis.com	vcrisi	NEWS	No	#N/A	DNS	#N/A	DNS	#N/A	DNS	#N/A	DNS	#N/A	DNS	#N/A
buscadorprimaria2023.com	Buscador primarias 2023	POLR	#N/A	DNS	#N/A	HTTPS/HTTP	#N/A	DNS	#N/A	DNS	#N/A	DNS	#N/A	DNS
d1zjwmfds04x7i.cloudfront.net	Buscador primarias 2023	POLR	#N/A	DNS	#N/A	DNS	#N/A	DNS	#N/A	DNS	#N/A	No	#N/A	No
d3lokqj5h9z9zs.cloudfront.net	Buscador primarias 2023	POLR	#N/A	DNS	#N/A	DNS	#N/A	DNS	#N/A	No	#N/A	No	#N/A	No
comisiondeprimariave.org	Comison primarias	POLR	#N/A	DNS	#N/A	DNS	#N/A	DNS	#N/A	No	#N/A	No	#N/A	No
hugocarvajal.com	hugocarvajal.com	POLR	DNS + HTTP/ HTTPS	HTTPS/DNS + HTTP	DNS	DNS	DNS	No	DNS	DNS	DNS	DNS	DNS	DNS

DOMINIO	SITIO	CATEGORIA	CANTV		Movistar		Digitel		Inter		Netuno		Supercable	
			2022	2023	2022	2023	2022	2023	2022	2023	2022	2023	2022	2023
www.lapatilla.com	la patilla	NEWS	DNS + HTTP/ HTTPS	DNS + HTTPS	DNS	DNS	DNS	DNS	DNS	DNS	DNS	DNS	DNS	DNS
liberal-venezolano.blogspot.com	liberal-venezolano.blogspot.com	NEWS	DNS + HTTP	DNS	DNS	DNS	DNS	DNS	DNS	DNS	DNS	DNS	DNS	DNS
maduradas.com	Maduradas	NEWS	HTTP/HTTPS	DNS	DNS	DNS	DNS	DNS	No	No	DNS	DNS	No	No
minuto30.com	Minuto 30	NEWS	DNS	DNS	DNS	DNS	DNS	DNS	DNS	DNS	DNS	DNS	DNS	DNS
www.minuto30.com	Minuto 30	NEWS	#N/A	DNS + HTTPS	#N/A	DNS	#N/A	DNS	#N/A	DNS	#N/A	DNS	#N/A	DNS
monitoreamos.com	Monitoreamos	NEWS	DNS + HTTP/ HTTPS	DNS + HTTPS	DNS	DNS	DNS	DNS	DNS	DNS	DNS	DNS	DNS	DNS
noticiaaldia.com	noticia al dia	NEWS	DNS + HTTP/ HTTPS	DNS + HTTPS	DNS	DNS	DNS	DNS	No	DNS	DNS	DNS	DNS	DNS
noticialdia.com	noticia al dia	NEWS	DNS + HTTP/ HTTPS	DNS + HTTPS	DNS	DNS	DNS	No	DNS	DNS	DNS	DNS	DNS	DNS
noticiasvenezuela.org	noticias venezuela	NEWS	DNS + HTTP/ HTTPS	No	DNS	DNS	DNS	DNS	DNS	DNS	DNS	DNS	DNS	DNS
noticias.com	Noticias.com	NEWS	#N/A	DNS	#N/A	HTTPS/DNS + HTTP	#N/A	DNS	#N/A	DNS	#N/A	DNS	#N/A	DNS
noticierodigital.com	noticiero digital	NEWS	#N/A	DNS	#N/A	No	#N/A	DNS	#N/A	No	#N/A	No	#N/A	No
www.noticierodigital.com	noticiero digital	NEWS	DNS + HTTP/ HTTPS	DNS	No	No	No	No	No	No	No	No	No	No
www.ntn24.com	ntn 24	NEWS	DNS + HTTP/ HTTPS	DNS + HTTPS	DNS	DNS	DNS	DNS	DNS	DNS	DNS	DNS	DNS	DNS
www.opinionynoticias.com	Opinion y Noticias	NEWS	#N/A	No	#N/A	HTTPS/HTTP	#N/A	No	#N/A	No	#N/A	No	#N/A	No
primerinforme.com	primer informe	NEWS	DNS	DNS	DNS	DNS	DNS	No	DNS	DNS	DNS	DNS	DNS	DNS
puntodecorte.com	Punto de corte	NEWS	DNS	DNS + HTTPS	DNS	DNS	DNS	DNS	DNS	DNS	DNS	DNS	DNS	DNS

www.xvideos.com	XVideos	PORN	HTTP	#N/A	DNS	#N/A	DNS	#N/A	DNS	#N/A	DNS	#N/A	DNS	#N/A
bravotube.tv	BravoTube	PORN	HTTP	#N/A	No	#N/A	No	#N/A	No	#N/A	No	#N/A	No	#N/A
www.pornhub.com	PornHub	PORN	HTTP	#N/A	DNS	#N/A	DNS	#N/A	DNS	#N/A	DNS	#N/A	No	#N/A
www.tube8.com	Tube8	PORN	HTTP	#N/A	No	#N/A	No	#N/A	No	#N/A	No	#N/A	No	#N/A
www.youporn.com	YouPorn	PORN	HTTP	#N/A	No	#N/A	No	#N/A	No	#N/A	No	#N/A	No	#N/A
coronavirusvenezuela.info	coronavirusvenezuela.info	PUBH	DNS + HTTP	DNS + HTTPS	DNS	DNS	DNS	DNS	HTTP	HTTP	DNS	DNS	HTTP	HTTP
medicos.presidenciave.org	medicos.presidenciave.org	PUBH	No	No	DNS	DNS	No	No	No	No	No	No	No	No
www.hidemyass.com	Hidemyass	VPN	No	No	No	No	No	No	No	No	DNS	DNS	No	No
psiphon.ca	Psiphon	VPN	DNS + HTTP/ HTTPS	DNS + HTTPS	DNS	DNS	DNS	No	DNS	DNS	DNS	DNS	DNS	DNS
tunnelbear.com	Tunnelbear	VPN	DNS + HTTP/ HTTPS	DNS + HTTP, HTTPS/DNS + HTTP	DNS	DNS	DNS	No	DNS	DNS + HTTP	DNS	DNS	DNS	DNS
api.tunnelbear.com	Tunnelbear	VPN	DNS + HTTP	DNS + HTTP, HTTPS/DNS + HTTP	DNS	DNS	No	No	No	No	DNS	DNS	DNS	DNS
Tunnelbear	VPN	DNS + HTTP	DNS + HTTP, HTTPS/DNS + HTTP	DNS	DNS	No	No							

Tabla con una lista de dominios bloqueados en 2022 y 2023 hasta la fecha de impresión.
Múltiples formas de bloqueo son posibles simultáneamente; los valores separados por comas denotan un cambio durante ese año.

DOMINIO	SITIO	CATEGORIA	CANTV		Movistar		Digitel		Inter		Netuno		Supercable	
			2022	2023	2022	2023	2022	2023	2022	2023	2022	2023	2022	2023
infodio.com	infodio.com	POLR	DNS	DNS	DNS	DNS	DNS	DNS	DNS	DNS	DNS	DNS	DNS	DNS
lavenezueladelencuentro.com	la venezuela del encuentro	POLR	#N/A	DNS	#N/A	DNS	#N/A	DNS	#N/A	No	#N/A	No	#N/A	No
www.maduradas.com	Maduradas	POLR	DNS + HTTP	DNS + HTTPS	DNS	DNS	DNS	DNS	DNS	DNS	DNS	DNS	No	No
www.mdivenezuela.org	MDI Venezuela	POLR	DNS + HTTP	DNS	No	DNS	No	DNS	No	DNS	No	No	No	DNS
presidenciave.com	presidenciave.com	POLR	HTTP/HTTPS	DNS + HTTPS	DNS	DNS	DNS	DNS	DNS	DNS	DNS	DNS	DNS	DNS
pvenezuela.com	pvenezuela.com	POLR	DNS	DNS	DNS	DNS	DNS	DNS	DNS	DNS	DNS	DNS	DNS	DNS
teleconsulta.presidenciave.org	teleconsulta.presidenciave.org	POLR	No	No	DNS	DNS	No	No	No	No	No	No	No	No
vamosbien.com	vamosbien.com	POLR	DNS + HTTP	DNS + HTTPS	No	No	No	No	No	No	No	No	No	No
vdebate.blogspot.com	vdebate	POLR	DNS	DNS	DNS	DNS	DNs	DNS	DNS	DNS	DNS	DNS	DNS	DNS
www.ventevenezuela.org	www.ventevenezuela.org	POLR	HTTP/HTTPS	HTTPS	No	No	No	No	No	No	No	No	No	No
venezuelaaidlive.com	venezuelaaidlive.com	POLR	No	No	DNS	DNS	DNS	DNS	DNS	DNS	DNS	DNS	DNS	DNS
robertopatino.com	roberto patiño	POLR	DNS	#N/A	DNS	#N/A	DNS	#N/A	DNS	#N/A	DNS	#N/A	DNS	#N/A
www.vamosbien.com	vamos bien	POLR	HTTP/HTTPS	#N/A	No	#N/A	No	#N/A	No	#N/A	No	#N/A	No	#N/A
hdzog.com	hdzog.com	PORN	HTTP	HTTP	No	No	No	No	No	No	No	No	No	No
www.petardas.com	www.petardas.com	PORN	HTTP	HTTPS	No	No	No	No	No	No	No	No	No	No
xhamster.com	XHamster	PORN	HTTP	#N/A	DNS	#N/A	DNS	#N/A	No	#N/A	DNS	#N/A	DNS	#N/A


ERROR
404
451
ERROR
404
451
ERROR
404
451
ERROR
404
451