WITHOUT RIGHTS

ON #INTERNETVE

ANNUAL REPORT ON THE STATE OF HUMAN RIGHTS ONLINE IN VENEZUELA

REPORT 2021

INTERNET BLOCKS
CENSORSHIP
CONNECTIVITY
DIGITAL ATTACKS

VE SIN FILTRO

VESINFILTRO.COM/2021

2I 2021**REPORT**

VESINFILTRO

Report2021

About VE Sin Filtro

VE Sin Filtro is a program run by the organization Venezuela Inteligente that uses technical criteria to monitor and document internet censorship and other threats to the exercise of human rights. The VE Sin Filtro program won LACNIC's FRIDA Award for Free and Open Internet.

It was launched in 2014 to help identify and avoid media censorship. VE Sin Filtro has pioneered the use of a combination of automatically produced network measurements, open source measurements, network traffic analysis, and open source research to investigate restrictions of human rights online.

VE Sin Filtro offers emergency assistance to civil society organizations, journalists, and independent media outlets that come under attack or are subjected to censorship, helping to resolve the incident, mitigate the impact of censorship, and document cases.

Introduction

Error messages are appearing with increasing frequency on the screens of Venezuelans who attempt to access websites that include news content. The practice of blocking these sites combined with precarious internet connections and reiterated interruptions in electricity service make normal browsing exceedingly difficult, thus limiting enjoyment of one of the activities that the United Nations has identified as a fundamental right: accessing the internet.

According to a 2016 resolution of the UN Council on Human Rights, all States have the duty to ensure internet freedom and security. As such, preventing citizens from freely accessing the internet is considered a human rights violation.

That resolution states that, “The same rights people have offline must also be protected online,” very especially those related to freedom of expression.

Online media censorship has grown exponentially since 2014. During the 2014 and 2017 protests in Venezuela, the most critical parties and news streaming services came under attack, as did their audiences. In 2018, internet censorship began to impact traditional media outlets, and more sophisticated mechanisms were used to block them.

There is a connection between the political reality and internet censorship, and that parallel explains the constant violation of digital rights in Venezuela. Recently, as the President began to face a crisis of legitimacy, platforms that had not previously been affected faced blocks, while news attacks became widespread.

New blocks were activated in 2021, and existing ones remained in place. For example, during the regional elections in November, VE Sin Filtro determined that over 56

luction

key web domains relevant to the election were blocked, which prevented users from accessing information, as traditional media outlets have disappeared or are subject to censorship.

Between January and December 2021, VE Sin Filtro found that 59 websites corresponding to at least 68 domains were blocked. Forty-five of these were media sites, eight belonged to portals that offer political content, four are designed to share multimedia content, three are run by human rights organizations, six had adult content, and two were VPN (Virtual Private Network) platforms used to avoid censorship.

During this period, blocks reappeared against media outlets that had been targeted in the past, including La Patilla, Caraota Digital, and Alberto News. Access to their alternative domains was restricted in 2021, and they ended up being blocked by Internet Service Providers (ISPs) that had previously allowed access to them.

Similarly, the websites of NGOs were blocked, including that of Acceso a la Justicia, thus escalating the levels of persecution of human rights activists and organizations that document the absence of guarantees and support victims.

VE Sin Filtro reported nearly 50 connectivity incidents in 2021. The most common cause of lack of internet connection was nationwide electric outages, especially in Andean states, particularly Táchira. These data are based on monitoring the performance of six internet service providers: the state-owned entity CANTV and private operators Inter, Movistar, Digitel, NetUno, and SuperCable.

Censorship Events

CENSORSHIP EVENTS

AMBUSHING THE MEDIA

6 February

The website Insight Crime was blocked on February 6. VE Sin Filtro found that the restrictions were imposed just days after the site published a report on homicide rates in Latin America that ranked Venezuela as the second most violent country in the region. CANTV executed an HTTP/HTTPS-type block. It was lifted in June 2021, and the webpage's domains (www.insightcrime.org and es.insightcrime.org) are not currently blocked.

25 May

The TeleSur Libre website promoted by Juan Guaidó was blocked on May 25 by all ISPs (Internet Service Providers), just one day after it launched. CANTV used DNS and HTTP/HTTPS-type blocks, while Inter, Movistar, Digitel, NetUno, and SuperCable used a DNS block.

29 May

The country's main internet providers began to block access to lapatilla.com on May 29. The block began with Movistar, Digitel, Inter, and SuperCable, and NetUno blocked it on June 1. CANTV has blocked La Patilla's main domain since before 2021. Connections to La Patilla's alternative domains -which are used instead of lapatilla.com- also have been blocked on CANTV using HTTP/HTTPS and DNS concurrently.

early june

In early June, at least two alternative domains of the news portal Caraota Digital (caraotadigital.xyz and caraotadigital.news) that had been used to avoid censorship were blocked. Access to Caraota Digital through its original domain, caraotadigital.com, was blocked in 2020. These new DNS-type blocks were used by all of Venezuela's private providers, but we have no data regarding precisely when the move took place.

Movistar also executed a DNS block of one of the alternative domains used by Alberto News. Digitel and SuperCable reactivated the block between June 28 and 29. Inter, NetUno, and CANTV have had it blocked since 2020.

9 May

SoundCloud, the largest audio hosting platform on the internet, was blocked by the private operators on May 9. Access has been restricted on CANTV since 2019. SoundCloud is used by news outlets as an alternative due to extensive blocks of webpages. The private providers' SoundCloud block affects the distribution of audio news capsules online as well as news reports from the Servicio de Información Pública (Public Information Service), Notiaudios from El Pitazo, the distribution of some podcasts, and other material.

19 October

On October 19, it was determined that the website hugocarvajal.com, a portal owned by Hugo "El Pollo" Carvajal, the former director of Venezuela's intelligence services, had been blocked. Carvajal had announced the relaunch of the website on his Twitter account just three days earlier. Venezuela's main internet provider, the state-owned company CANTV, implemented an HTTP/HTTPS block with SNI filter and DNS block. Movistar and Digital used a DNS block.

14 November

The website venezuelazonagris.com, which is part of a new investigative project developed by journalist Ibéyise Pancheco, was blocked on November 14, just three days after it was published. The country's main internet providers -CANTV, Inter, NetUno, Movistar, and Digitel- blocked the site. The state-owned company used an HTTP/HTTPS block with SNI filter along with a DNS block. The other providers only used a DNS block.

The table below shows the domains of webpages with news or political content that were blocked in 2021 or that started or ended the year facing such restrictions. It also shows the type of block applied by each operator.

Domain	Category	CANTV	Movistar	Digitel	Inter	Netuno	SuperCable
www.insightcrime.org	NEWS	HTTP/HTTPS*	No	No	No	No	No
es.insightcrime.org	NEWS	HTTP/HTTPS*	No	No	No	No	No
soundcloud.com	MULTIMEDIA	DNS + HTTP/HTTPS	DNS	DNS	No	DNS	DNS
telesurlibre.com	NEWS	DNS + HTTP/HTTPS	DNS	DNS	DNS	DNS	DNS
albertonews.com	NEWS	DNS + HTTP/HTTPS	DNS	DNS	DNS	DNS	DNS
www.caraotadigital.net	NEWS	HTTP/HTTPS	DNS	DNS	DNS	DNS	DNS
caraotadigital.xyz	NEWS	DNS + HTTP/HTTPS	DNS	DNS	DNS	DNS	DNS
caraotadigital.news	NEWS	DNS + HTTP/HTTPS	DNS	DNS	DNS	DNS	DNS
lapatilla.com	NEWS	DNS + HTTP/HTTPS	DNS	DNS	DNS	DNS	DNS
hugocarvajal.com	POLITICS	DNS + HTTP/HTTPS	DNS	DNS	DNS	DNS	DNS
venezuelazonagris.com	NEWS	DNS + HTTP/HTTPS	DNS	DNS	DNS	DNS	DNS
www.2001.com.ve	NEWS	HTTP/HTTPS	No	No	No	No	No
alnavio.com	NEWS	DNS + HTTP/HTTPS	DNS	DNS	DNS	DNS	DNS
www.aporrea.org	NEWS	HTTP/HTTPS	No	No	No	No	No
armando.info	NEWS	DNS + HTTP/HTTPS	DNS	DNS	DNS	No	DNS
dolartoday.com	NEWS	DNS	DNS	DNS	DNS	DNS	DNS
dolartoday.info	NEWS	DNS	DNS	DNS	DNS	DNS	DNS
dolartoday.org	NEWS	DNS	DNS	DNS	DNS	DNS	DNS
bit.ly/venezuela911	NEWS	No	HTTP	No	No	No	No
efectococuyo.com	NEWS	HTTP/HTTPS	No	No	No	No	No
elpitazo.net	NEWS	DNS	DNS	DNS	DNS	DNS	DNS
www.eltiempo.com	NEWS	DNS	DNS	DNS	DNS	DNS	DNS
evtvmiami.com	NEWS	HTTP/HTTPS	No	No	No	No	No
diariolaregion.net	NEWS	DNS + HTTP/HTTPS	DNS	No	DNS	DNS	DNS
www.infobae.com	NEWS	DNS + HTTP/HTTPS	DNS	DNS	DNS	DNS	DNS
infodio.com	NEWS	DNS	DNS	DNS	DNS	DNS	DNS
lamananadigital.com	NEWS	DNS + HTTP/HTTPS	No	No	No	No	No
maduradas.com	NEWS	HTTP/HTTPS	DNS	DNS	No	DNS	No
minuto30.com	NEWS	DNS	DNS	DNS	DNS	DNS	DNS
monitoreamos.com	NEWS	DNS + HTTP/HTTPS	DNS	DNS	DNS	DNS	DNS
noticialdia.com	NEWS	DNS + HTTP/HTTPS	DNS	DNS	DNS	DNS	DNS
noticiaaldia.com	NEWS	DNS + HTTP/HTTPS	DNS	DNS	No	DNS	DNS
noticiasvenezuela.org	NEWS	DNS + HTTP/HTTPS	DNS	DNS	DNS	DNS	DNS
www.el-nacional.com	NEWS	HTTP/HTTPS	No	No	No	No	No
www.noticierodigital.com	NEWS	DNS + HTTP/HTTPS	No	No	No	No	No
www.ntn24.com	NEWS	DNS + HTTP/HTTPS	DNS	DNS	DNS	DNS	DNS
pvenezuela.com	POLITICS	DNS	DNS	DNS	DNS	DNS	DNS
presidenciave.com	POLITICS	HTTPS/HTTP	DNS	DNS	DNS	DNS	DNS
puntodecorte.com	NEWS	DNS	DNS	DNS	DNS	DNS	DNS
reddit.com	MULTIMEDIA	No	DNS	No	No	No	No
runrun.es	NEWS	DNS	No	No	No	DNS	No
livestream.com	MULTIMEDIA	DNS	No	DNS	DNS	DNS	DNS
sumarium.es	NEWS	HTTP/HTTPS	No	No	No	No	No
sunoticiero.com	NEWS	DNS + HTTP/HTTPS	DNS	DNS	DNS	DNS	DNS
venezuelaaidlive.com	POLITICS	No	DNS	DNS	DNS	DNS	DNS
www.venezuelaaldia.com	NEWS	No	DNS	DNS	DNS	DNS	No
www.ventevenezuela.org	POLITICS	HTTPS/HTTP	No	No	No	No	No
vivoplay.net	NEWS	HTTPS	DNS	DNS	DNS	DNS	No
vpitv.com	NEWS	DNS + HTTP/HTTPS	DNS	DNS	DNS	DNS	DNS
zello.com	MULTIMEDIA	DNS	HTTP	DNS	No	No	No
alekboyd.blogspot.co.uk**	NEWS	DNS	DNS	DNS	No	DNS	DNS
alekboyd.blogspot.com**	NEWS	No	DNS	DNS	No	DNS	DNS
robertopatino.com**	POLITICS	DNS	DNS	DNS	DNS	DNS	DNS
www.vamosbien.com**	POLITICS	HTTPS/HTTP	No	No	No	No	No
www.vcrisis.com**	NEWS	DNS	DNS	DNS	DNS	DNS	DNS
vdebate.blogspot.com**	POLITICS	DNS	DNS	DNS	DNS	DNS	DNS

* A block that was disabled before the end of the year

** Obsolete domain

ACTIVISTS UNDER ATTACK

8

march

The webpage of Acceso a la Justicia, a human rights NGO that specializes in monitoring justice administration and the rule of law in Venezuela, was blocked beginning on April 8. The measure prevented CANTV users from entering accesoalajusticia.org.

Users can only manage to get around the HTTP/HTTPS block implemented by CANTV if they have a VPN. Notably, unknown actors attempted to silence the Acceso a la Justicia website in 2020 as well. It was taken offline after its hosting service provider received malicious DMCA takedown requests based on bogus copyright claims designed to cause the entity to lose its web hosting. These were eventually discredited after mediation with the hosting provider.

This HTTP and HTTPS block is classified as an application layer block, requiring deep packet inspection to selectively block communication with the server when this webpage is being requested.

The NGO Mi Convive's webpage has been blocked since 2020. These actions constitute yet another attack on human rights in Venezuela, as they limit the right to freedom of expression and information and limit the right to freedom of peaceful association in a context of extensive censorship of the online and traditional press as well as threats and persecution of civil society organizations.

Domain	Category	CANTV	Movistar	Digitel	Inter	Netuno	SuperCable
www.accesoalajusticia.org	Human Rights	HTTP	No	No	No	No	No
miconvive.com	Human Rights	DNS	DNS	DNS	DNS	DNS	DNS
www.change.org	Human Rights	HTTP	DNS	DNS	DNS	DNS	DNS

VESINFILTRO

Adult Content

LIMITATIONS ON ADULT CONTENT

2 march

On March 2, CANTV censored access to sites with pornographic or adult content using an HTTP block. Seven days later, on March 9, Movistar, NetUno, Inter, and Digitel applied a DNS block. SuperCable did the same on March 29.

Six pornography websites have been blocked in Venezuela by the main internet providers, including some of the best-known portals for this type of content. CANTV blocked all six sites, and the rest of the operators blocked at least one of them. This is not the first time adult content has been censored in Venezuela. Specifically, CANTV has blocked and unblocked multiple pornography pages in the past.

These sites were blocked for the last time when CANTV reactivated some HTTP/HTTPS restrictions that had been lifted following a fire in one of its facilities that impacted its capacity to censor.

Domain	Category	CANTV	Movistar	Digitel	Inter	Netuno	SuperCable
www.xvideos.com	PORNOGRAPHY	HTTP	DNS	DNS	DNS	DNS	DNS
xhamster.com	PORNOGRAPHY	HTTP	DNS	No	No	DNS	DNS
www.pornhub.com	PORNOGRAPHY	HTTP	DNS	No	DNS	No	No
bravotube.tv	PORNOGRAPHY	HTTP	No	No	No	No	No
www.youporn.com	PORNOGRAPHY	HTTP	No	No	No	No	No
www.tube8.com	PORNOGRAPHY	HTTP	No	No	No	No	No

Other Forms of Internet Censorship

News outlets and civil society are also subjected to other types of attacks in Venezuela, including online intimidation and harassment. Attacks on web servers have also been observed, including Denial of Service attacks where the server is saturated and stops responding to legitimate requests.

Pseudo-legal strategies have been used to intimidate or force sites to remove content, including malicious DMCA takedown requests, a technique that was almost unheard of in Venezuela prior to 2021. This mode includes asking that content be taken offline or the wholesale removal of a website or account from hosting providers, other services or online platforms based on supposed copyright violations that turn out to be false. They also include baseless legal threats to intimidate victims.

This comes in addition to the existing environment of intimidation and pressure that impacts journalists, activists and human rights defenders. As other organizations have reported, these individuals and entities risk being subject to offline attacks as well as prosecution, illegal detentions, and even torture due to their work and legitimate exercise of freedom of expression online.

VESINFILTRO

Censorship

CENSORSHIP OF ANTI-CENSORSHIP TOOLS

Venezuelans must use various evasion tools and strategies to access reliable information and avoid surveillance. The most effective of these has been VPN services that allow users to hide users' traffic and get around internet blocks despite attempts to limit them.

Changing a device's default DNS servers is another common approach, but it does not work for many blocked sites, particularly with CANTV, which frequently uses more sophisticated blocking techniques.

Public reports about multiple blocked websites have made Venezuelans more aware of the use of VPNs as a tool for getting around censorship. Since this information has become public, operators have begun to put up obstacles to limit the use of these tools.

The 2021 TunnelBear block remained in place on Venezuela's main providers. Its main website, tunnelbear.com, has experienced simultaneous DNS and HTTP/HTTPS blocks by CANTV since 2019. The rest of the operators introduced a DNS block on August 20, 2020. The Digitel block was lifted from March 7 to October 12, 2021.

The VPN can currently be downloaded from alternative URLs and from app stores on various operating systems and works fairly smoothly. Although the TunnelBear VPN has continued to be functional, new users could not be registered during part of 2021 because of the block. This was resolved following discussions with the provider. However, the password change function is still disabled because this must be completed on the main tunnelbear.com domain, which is currently blocked.

Venezuela's six main providers have blocked Psiphon's main domain (psiphon.ca) since August 2020. The restriction remained in place for all of 2021. CANTV used HTTP/HTTPS and DNS. The other ISPs only used a DNS block.

These block events prevent users from accessing the Psiphon website to download the PC version of the software, but they do not affect the VPN's functionality or user experience.

VE Sin Filtro recommends that users use Psiphon and TunnelBear. The blocks on them have inspired campaigns recommending them and teaching users how to use them.

Tor is a well-known tool that provides a high level of anonymity for internet browsing and helps users get around censorship. VE Sin Filtro found an increase in the number of bridges and authority directories that cannot be accessed from CANTV.

This means that an effort is being made to block Tor connections in Venezuela, but that it is not very effective. According to measurements conducted over the past few months, 70 to 80% of Tor authority directories are blocked at any point in time by the state-owned company CANTV.

This censorship of Tor is based on a TCP block of these IPs or known IPs and is similar to what happened in 2018. Many publicly known bridges that had not been included have now been blocked.

Domain	Category	CANTV	Movistar	Digitel	Inter	Netuno	SuperCable
psiphon.ca	VPN	DNS + HTTP/HTTPS	DNS	DNS	DNS	DNS	DNS
tunnelbear.com	VPN	DNS + HTTP/HTTPS	DNS	DNS	DNS	DNS	DNS

14I 2021**REPORT**

VESINFILTRO

CONNECTIVITY AND INTERNET SERVICE AVAILABILITY

VESINFILTRO

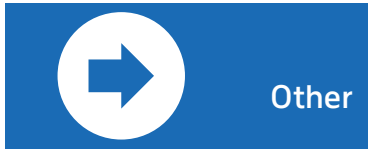
2021**REPORT I**15

Connectivity

VE Sin Filtro analyzed Internet connectivity levels in Venezuela. Its research focused on CANTV, Digitel, Inter, Movistar, Net Uno, and SuperCable.

This allowed us to identify incidents involving a drop in the usual connectivity values at the national and regional levels. These drops are large scale incidents. As such, localized low-magnitude cases are not included in the report. Another factor to consider is that the measurements are the number of network segments /24 normalized. It is not possible to document the cases of populations in which the operators that we monitor do not have an active connection service for a variety of reasons.

The main causes of these incidents are:



Decreases in connectivity were categorized according to the magnitude of the percentage of the connectivity level:

CRITICAL

Critical: 0-50%

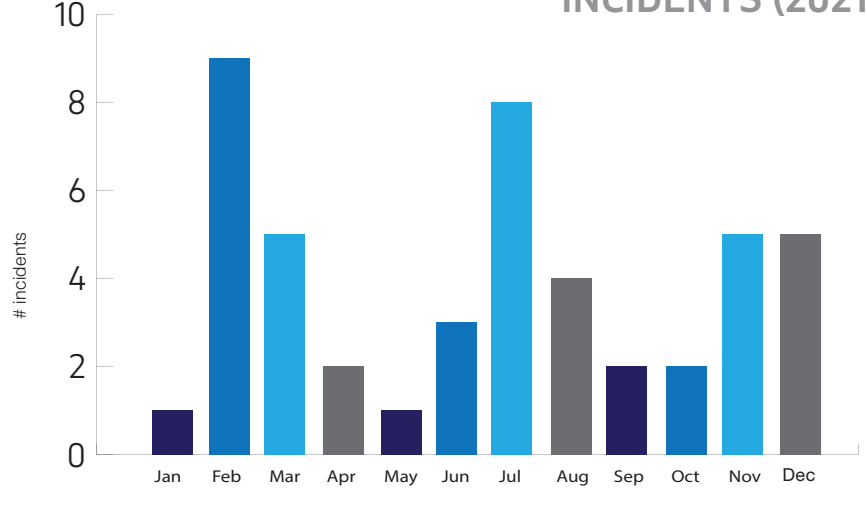
SERIOUS

Serious: 51-80%

MILD

Mild: A drop that is not lower than 80% but coincides with a clear connectivity decrease event in various states.

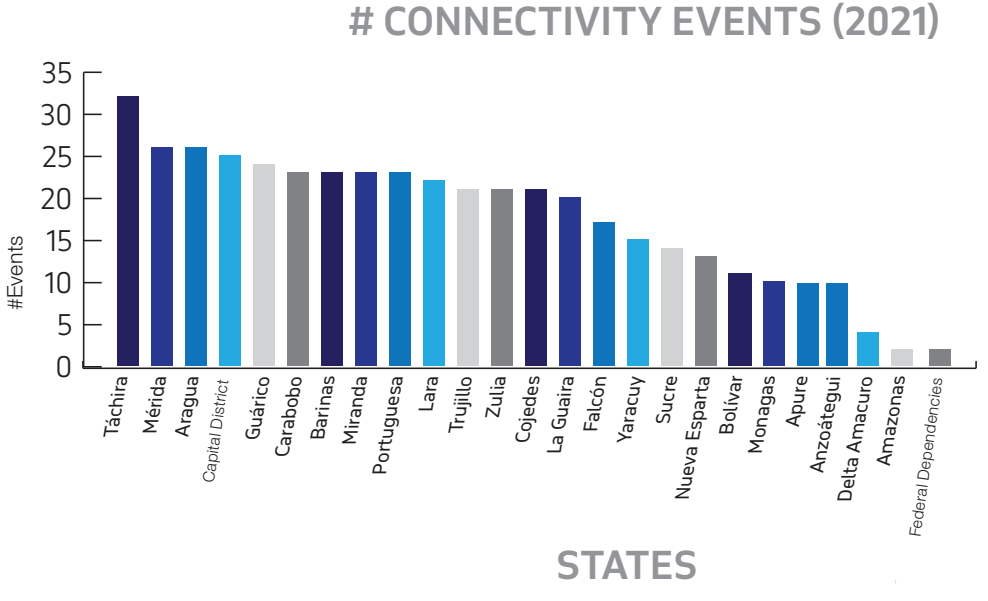
MONTHLY CONNECTIVITY INCIDENTS (2021)



VE Sin Filtro reported 47 internet connectivity decrease events in 2021. February was the month with the most cases (9).

Connectivity Incidents

The 47 national connectivity incidents had an impact on one or more states simultaneously. In terms of our methodology, these are the incidents that we call events. In this regard, the incidents for 2021 were assessed based on their impact on the entire country, which means that there were 454 regional events. Thirty-two of these events affected the state of Táchira, while Mérida, Aragua, and the Capital District presented 26 events each. Guárico had 25 events, and the rest of the states had between two and 24.



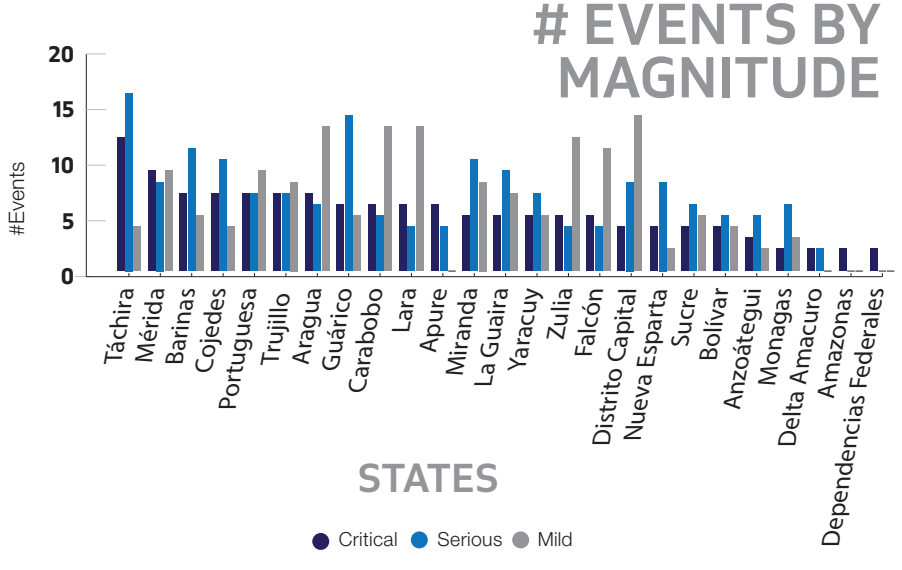
VESINFILTRO

Events by Incident Magnitude

The drop in connectivity levels compared to usual levels was characterized according to their magnitude, identifying critical, serious, and mild events. Táchira had the largest number of critical events (16) as well as the largest number of serious (16) and mild (4) events. It is followed by Mérida (9 critical) and Barinas, Cojedes, Portuguesa, Trujillo, and Aragua (7 critical). The rest of the states had between six and 12 critical events.

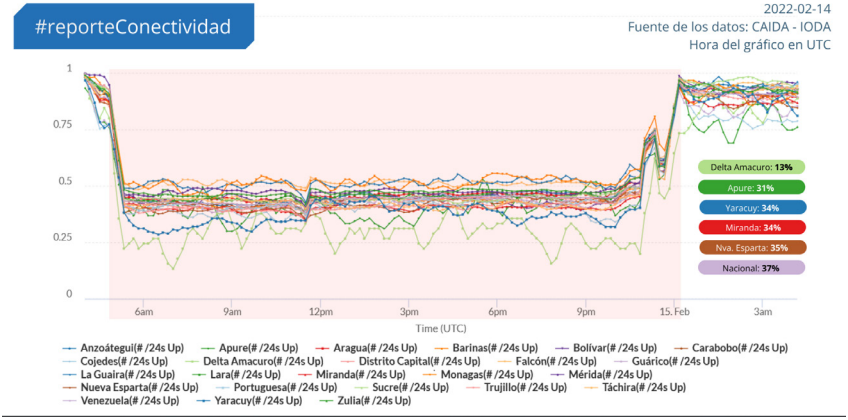
Most of the events were serious (166 total), followed by 154 mild events and 132 critical events nationally.

States	Critical	Serious	Mild	# Events
Táchira	12	16	4	32
Mérida	9	8	9	26
Barinas	7	11	5	23
Cojedes	7	10	4	21
Portuguesa	7	7	9	23
Trujillo	7	7	8	22
Aragua	7	6	13	26
Guárico	6	14	5	25
Carabobo	6	5	13	24
Lara	6	4	13	23
Apure	6	4	0	10
Miranda	5	10	8	23
La Guaira	5	9	7	21
Yaracuy	5	7	5	17
Zulia	5	4	12	21
Falcón	5	4	11	20
Capital District	4	8	14	26
Nueva Esparta	4	8	2	14
Sucre	4	6	5	15
Bolívar	4	5	4	13
Anzoátegui	3	5	2	10
Monagas	2	6	3	11
Delta Amacuro	2	2	0	4
Amazonas	2	0	0	2
Federal Dependencies	2	0	0	2



Events by Outage Type

With regard to the origin of the incidents, VE Sin Filtro identified blackouts or brownouts; failures caused by ISPs, mostly due to fiber optic cable outages or undefined internal service issues; and “others,” which are incidents of unknown origin.



60%
Electrical outages

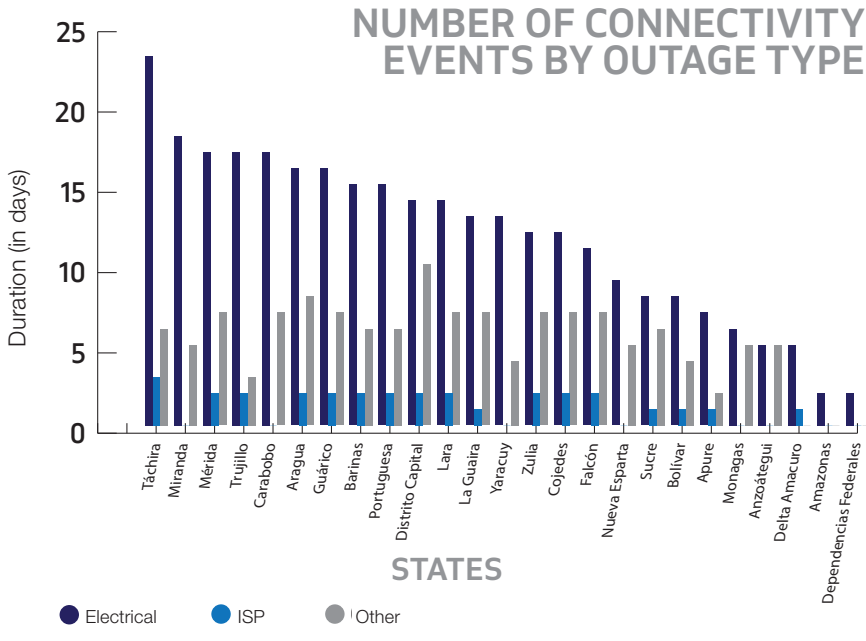
19h20m

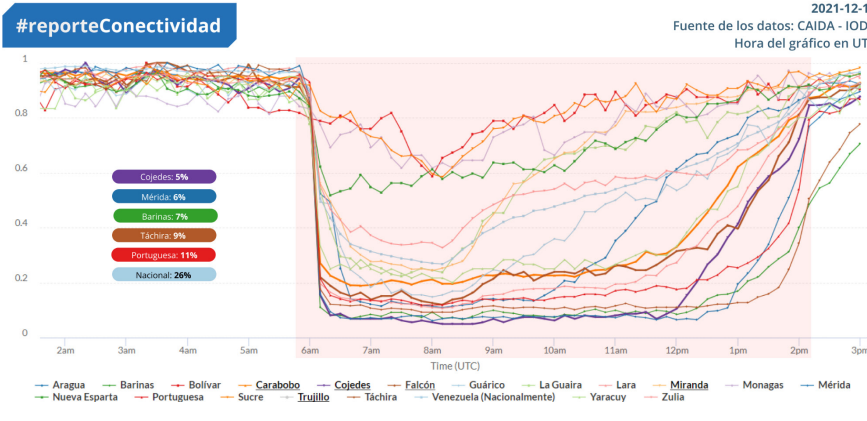
20
States

Sixty percent of the incidents identified in 2021 were due to electrical outages. If we look at the incidents regionally, there were 293 events in total, and Táchira had the largest number of them. Twenty-three of the events there were due to electrical outages. The other states that had the highest numbers of incidents were Miranda (18) and Carabobo, Mérida, and Trujillo (17). The others had between two and 16 events over the course of the year.

One of the events reported due to electrical outages took place on February 14. A blackout caused a decrease in connectivity levels in 23 states for 19 hours and 20 minutes. The incident began at 12:50 a.m. The lowest percentage registered nationally was 37% compared to normal levels. This qualifies as a critical drop in connectivity. Another 23 events presented a level of connectivity of between 0 and 50% of normal levels.

In late 2021, on December 17, there was a national blackout that has officially been considered an “attack on the electric system.” At least 20 states were left without electricity. The states that suffered the most serious impacts were Cojedes, Mérida, Barinas, Táchira, and Portuguesa, with connectivity levels of between 5 and 11% starting at 1:00 a.m. and lasting for eight hours. Nationally, connectivity levels reached 26%.



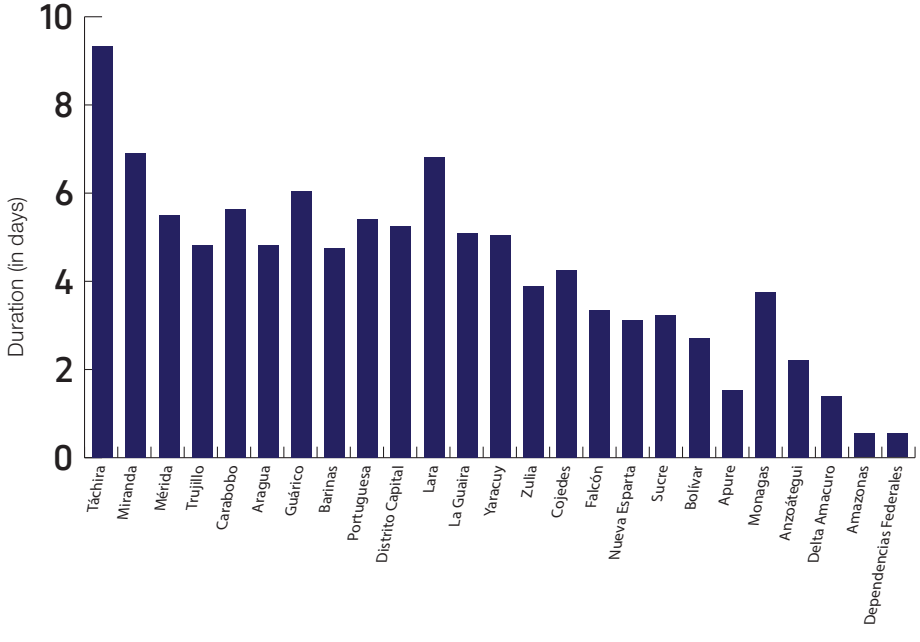


The incidents identified due to operator or service provider failure represent 17% of the total. Táchira again presented the largest number of cases (3). Incidents due to other causes represent 39% of the total. The Capital District had the highest number of cases (10).

Outages by Incident Duration and Event

The duration of total incidents presented within the national territory was 13 days and two hours. Regionally, Táchira is again the state with the longest connectivity outages (9 days, 8 hours and 20 minutes) followed by Mérida (6 days, 22 hours) and Trujillo (6 days, 19 hours and 50 minutes). The states that were impacted by connectivity outages for the longest amount of time are in the Andean region. The other states were impacted for between 13 hours and six days.

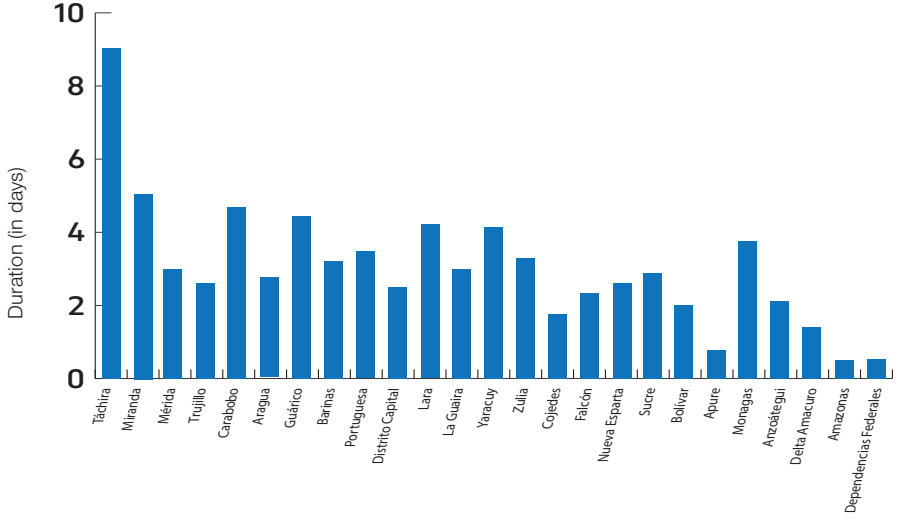
DURATION OF CONNECTIVITY EVENTS (2021)



Duration of Critical and Serious Incidents

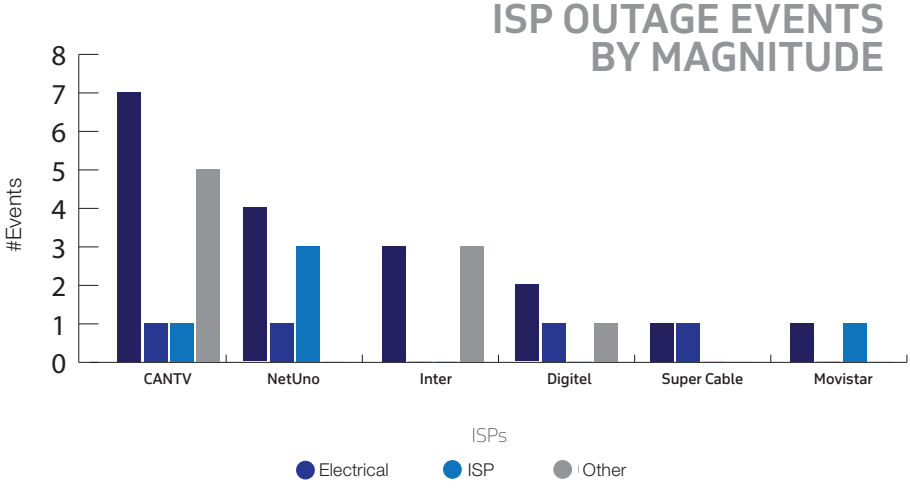
The states with the highest total amount of time impacted by critical and serious incidents are Táchira (7 days, 10 hours, and 10 minutes), Mérida and Trujillo (5 days and 16 hours), and Guárico (4 days, 17 hours, and 40 minutes). The rest of the states were impacted for between 13 hours and four days.

DURATION OF CRITICAL AND SERIOUS EVENTS (2021)

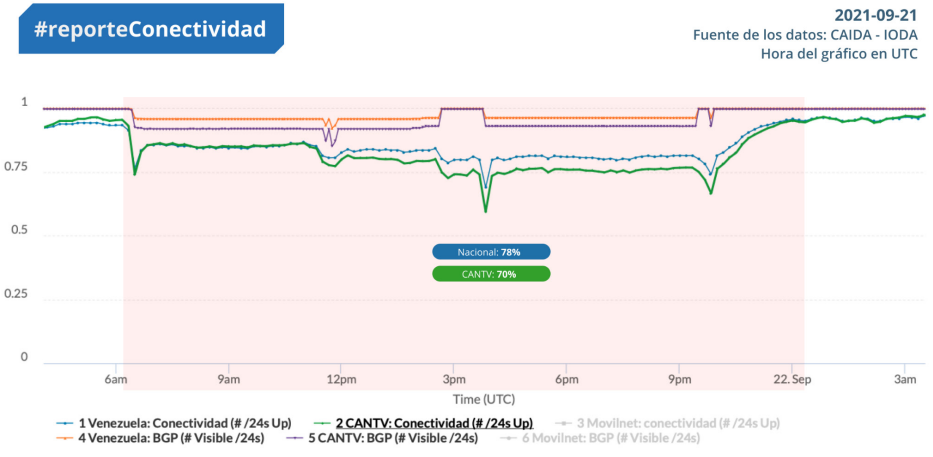


ISP Outage Incidents by Magnitude

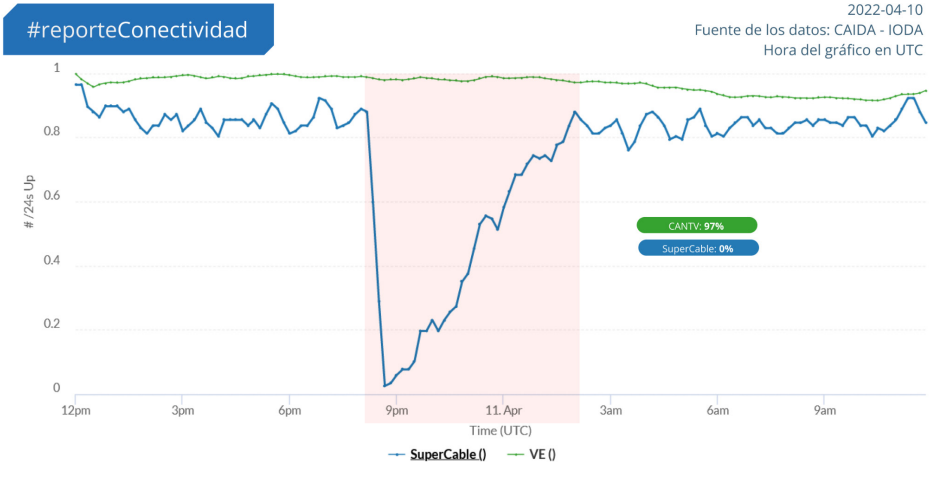
We have a total of eight incidents due to ISP outages representing 17% of the total outages. CANTV had the highest number of incidents (7 events: 1 critical, 1 serious, 5 mild) followed by NetUno (4 events: 1 critical and 3 serious), Inter (3 events), and Digitel. The ISP with the fewest events was Movistar, with one serious event.



On September 21, the state-owned entity CANTV reported that internet service was impacted by a triple cut of fiber optics that impacted the following regions: the Central Region, Los Llanos, the Western Central Region, the Western Region, and the state of Amazonas. VE Sin Filtro determined that the incident began at 2:30 a.m. and lasted for 17 hours. CANTV connectivity dropped up to 76% nationwide compared to their normal levels. The state that experienced the greatest impact was Táchira, where connectivity dropped to 49%, making this a critical event.

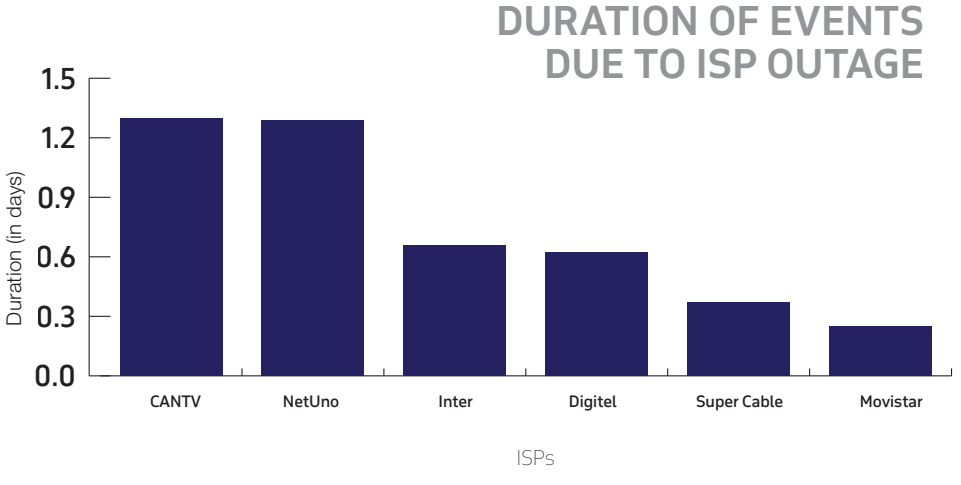


Another incident caused by ISP outages took place on April 10. A drop in connectivity through the provider SuperCable was detected. Connectivity levels reached 0%. The incident began at 4:00 p.m. and lasted for six hours.



ISP Outage Duration

If we take the duration of all ISP failure incidents together, the state-owned ISP CANTV has a total of one day, 7 hours and 20 minutes. It is followed by NetUno, with one day, 7 hours. Inter and SuperCable placed third, with 16 hours, and finally Movistar and Digitel had 15 and nine hours, respectively.



Phishing and Platform Account Theft

WhatsApp

VE Sin Filtro has observed an alarming increase in the number of phishing cases on WhatsApp over the past few years. While it is difficult to obtain real data on the scope of this phenomenon in Venezuela, we can report that we assisted more journalists, activists, and members of civil society who were impacted by these attacks in 2021 than we had in previous years.

Identity theft through WhatsApp has unfortunately become common, and all users run the risk of being the victim of this type of attack. The most frequently used method by far is WhatsApp authentication code theft through social engineering, which allows perpetrators to access victims' accounts. The attackers trick their victims by posing as customer support staff or another official in order to get them to divulge their WhatsApp access code in a text message.

The individuals responsible for this type of attack generally plan to pose as the victim to try to obtain money from their contacts. Attackers usually ask for loans or claim to engage in fake currency exchange operations in order to defraud other WhatsApp users.

There has also been an increase in direct attacks on journalists and NGOs.

The case of one NGO was particularly alarming, as it lost control of the WhatsApp account that it used to communicate with human rights

victims via the application. Unlike the cases we usually see, none of the users had been tricked or subjected to a phishing attack. This incident was probably perpetrated by or in coordination with State agents, which is not usually the case with fraudsters or other types of attackers. The incident occurred while Venezuela was being investigated by the International Criminal Court Prosecution Service and the UN Council on Human Rights was working on its fact-finding mission.

Instagram

While WhatsApp phishing cases are much more common, we have provided support to individuals who lost access to their Instagram accounts due to these attacks. Users with a large number of followers are especially vulnerable, as their accounts are very valuable to malicious actors who could try to steal them and sell them to third parties.

We conducted an exhaustive investigation into a case of phishing that impacted a public figure from the health sector who had hundreds of thousands of followers on Instagram in January and February of 2021. The account was eventually recovered thanks to the organization's efforts.

In general, the modus operandi observed in that case and most of the cases that we have been involved with is as follows:

The attackers send direct messages through Instagram to accounts that they consider valuable, posing as customer support staff working for the social media outlet.

They offer to verify the account (adding the blue verification symbol) if the person completes an online form. They also trick users with messages related to false copyright claims.

The form asks for the Instagram username and password, telephone number, and other details. It is hosted online under a domain designed to look official by imitating the brand's look.

The attackers take control of the account by changing the password, recovery email, and in some cases the name of the account.

They contact the victim through the information that they provided on the form and demand money from them in exchange for allowing them to recover the account. In other cases, the account is sold to a third party without any further communication with the victim.

It is important to note that all of the information obtained during our investigation was duly reported in an effort to ensure that others do not become victims of the same attack.

Access

Internet Access

The most recent figures from the National Telecommunications Commission of Venezuela (CONATEL) estimated internet penetration to be 53.66% nationally by the end of 2020. Residential internet penetration was 27.29%.

Available sources on internet penetration in Venezuela tend to differ by wide margins and use different methodologies. In February 2021, the Venezuelan Public Services Observatory estimated that just 34.2% of the population had fixed internet service, while 73% had mobile internet service. The same organization reported fixed internet penetration of 36.1% (a six percentage point improvement) in February 2022 and stated that mobile internet penetration stood at 83.7% (up 15 percentage points). Datareportal figures suggest that the improvement was just two percentage points in 2021.

Given the access that we have to internet provider data and difficulties related to these estimates, we can use CONATEL figures as the main reference and can estimate that the variation in internet penetration that occurred in 2021 was an increase of between two and 15 percentage points, taking the extreme values of change reflected by other sources with more up-to-date data.

In regard to user distribution, the CONATEL report for the last quarter of 2020 shows precarious and unequal internet access in the country. This also represents a violation of the population's human rights (association,

healthcare, identity, information, education, and others). The ten states with the lowest levels of penetration are Amazonas, Apure, Sucre, Delta Amacuro, Guárico, Falcón, Trujillo, Yaracuy, Zulia, and Portuguesa.

State	Internet Penetration Source: CONATEL, 2020.
Amazonas	14.79%
Apure	23.5%
Delta Amacuro	28.38%
Sucre	28.19%
Guárico	31.24%
Falcón	31.55%
Trujillo	32.43%
Yaracuy	32.43%
Zulia	36.58%
Portuguesa	35.13%
Monagas	36.35%
Bolívar	41.55%
Barinas	41.57%
Mérida	44.22%
Lara	50.69%
Táchira	52.29%
Anzoátegui	53.66%
Carabobo	54.37%
Aragua	57.75%
La Guaira	62.03%
Nueva Esparta	70.41%
Capital District	100.93%
Miranda	103.57%

During 2021, private operators invested the most in large cities where not all users have internet access, but penetration is notably higher. We believe that the states that had the internet lowest penetration rates in late 2020 will continue to present said levels for 2021.

Internet Speed

Venezuela has the second slowest internet connection speed in the region and one of the slowest in the world. This is in spite of the connection speed offered by new internet services at a “premium” price in some markets.

The internet connection speed and other performance factors determine whether users can use the internet in certain ways. A slow or unstable connection seriously limits the exercise of the right to work, education, communication, and expression by making it impossible for someone to collaborate with peers or colleagues, share content, interact in real time, and engage in other uses of this resource.

Download speed determines how long it takes to download work, school or university documents, and may even make it impossible to do so. It may also prevent users from watching videos online with sufficient quality, which is critical for distance learning when the student needs to be able to hear, see images or look at the blackboard. It also may limit the user’s ability to access audiovisual content in real time, such as news or live online classes.

The upload speed is critical for generating and sharing content, participating in videoconferences and interactive classes, and sharing multimedia content. It is especially critical for sharing live video. An individual’s ability to engage in Internet uses related to entertainment, work, education, and freedom of expression depends on having adequate broadband.

According to OOKLA, the median download speed during 2021 was between 3.34 and 7.21 Mbps. This is the speed at which a user can view webpages and consume online content. The upload speed was between

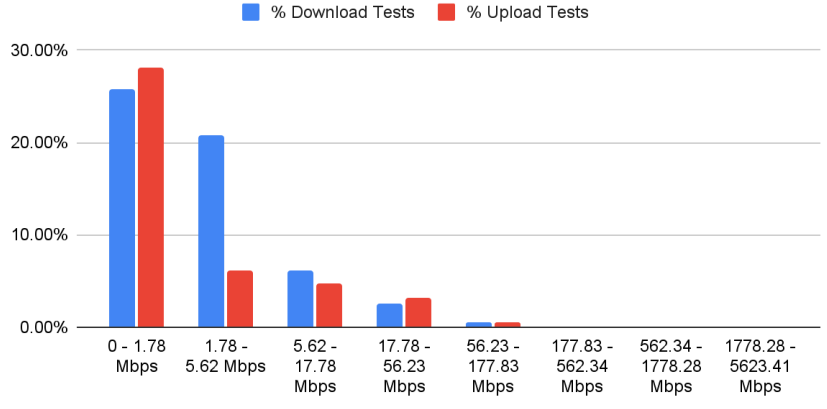
0.74 and 2.41 Mbps, which is what we use to upload a video, appear in a video conference or engage in similar activities.

OOKLA data are based on the users who visit its webpage to determine their real internet speed. Due to the fact that it is not a random sample, but a group selected based on page use and the technical methodology, one can assume that these figures are optimistic.

M-Lab places the average internet speed in Venezuela at between 1.03 and 1.59 Mbps for downloading and between 1.23 and 1.82 Mbps for uploading using the single traffic thread test. M-Lab's methodology represents the best connection performance for individual clients, but the speed indicators are lower than expected in many real cases, where multiple downloads are taking place simultaneously.

DENSITY OF RESULTS OF SPEED TESTS

% of all Venezuela tests in 2021 by speed. Source: M-Lab.)



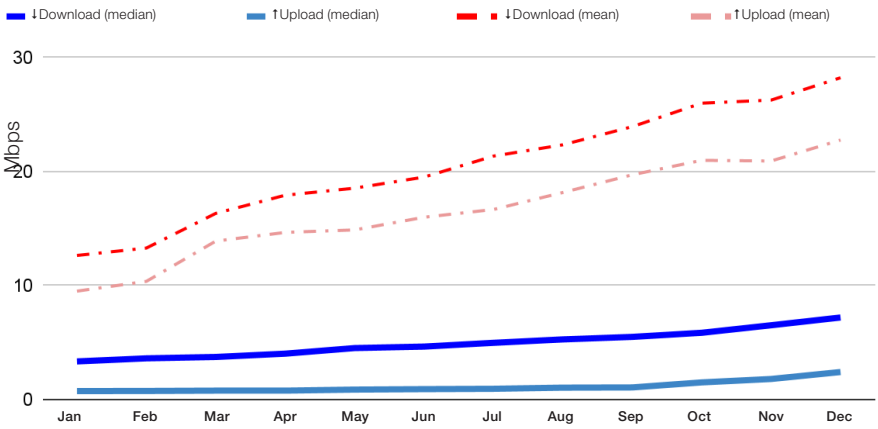
In April 2021, half of Venezuela's internet users had that speed according to OOKLA data. This is progress, but many people continue to have sub-par connections. In some countries, the minimum broadband speeds are 10.25 to 50 Mbps.

We have observed gradual increases in internet speed in Venezuela since mid-2020, but these improvements do not benefit all Venezuelans. Increased connectivity tends to benefit the few who are lucky enough to live in an area with coverage and have the ability to pay for new "premium" internet services, typically in dollars.

The M-Lab figures clearly show that the vast majority of speed tests are in the lower part of the results. This shows that the majority of Venezuelans access low-speed internet, while a minority enjoys much faster connection speeds.

FIXED INTERNET SPEED

Source: Venezuela's Fixed Broadband Internet Speeds -Ookla



The gap between those who have internet with speeds that allow them to comfortably use this resource and those who do not has grown. This compromises their right to fully participate in society. The growing divergence between median and mean speed reflects this distancing.

Mean speed is an average that includes the influence of small groups with much higher values than the majority, moving the average significantly, even if the vast majority does not undergo a change. The median speed is the point that half the population is above and half the population is below. This does a much better job of reflecting the experience that a Venezuelan might have.

Recommendations

Recommendations

FOR USERS

Use a VPN to access blocked or sensitive sites

We recommend having at least one VPN installed and tested on personal devices like cell phones and computers, even if you don't plan to use them right away.

The VPN we recommend is Psiphon, but TunnelBear is also a solid option that is very easy to use. You can use the following alternative links to download them in Venezuela. As of the date of publication of this report, they have not been blocked.

Psiphon

psiphon3.com
Android: Play Store
iOS: Apple App Store
Proxy: https://58685.info
E-mail: get@psiphon3.com

Tunnelbear

tuneloso.com
Android: Play Store
iOS: Apple App Store

We recommend using a trustworthy VPN, especially when you access websites with political content or participate in online activities that may lead to you becoming the target of persecution. A VPN also allows you to access blocked websites and media outlets.

CHANGE YOUR DNS CONFIGURATION

Changing the DNS server in your device's configuration may be a promising idea as long as you are aware that this will not help you to avoid all blocks in Venezuela and will not protect you from the advanced DNS manipulations that have been used in Venezuela.

VE Sin Filtro has a guide to changing the DNS configuration on your device. You can find it here.

Prevent account theft and unauthorized access

Use safe passwords that are impossible to guess and use a different one for each service that you use. To make it easier to use strong and unique passwords, we suggest utilizing a password manager to access your accounts safely. These tools allow users to generate random passwords and eliminate the need to memorize them.

We offer a video that explains the importance of safe passwords and best practices on the YouTube channel of our project Conexión Segura (Safe Connection).

Activate two-factor authentication. This involves introducing a second type of authentication apart from the password to access Internet service accounts, adding an extra layer of protection.

The temporary code sent via SMS is a popular method, but we recommend apps like Google Authenticator, Authy or a physical security key.

FOR THE STATE

Strictly adhere to international human rights standards to guarantee the exercise of human rights in the digital ecosystem without fear of retaliation, surveillance or censorship.

Suspend the abusive practice of blocking internet for news outlets, communication tools, apps, and other websites, as such practices go against freedom of expression, association, opinion, and information.

Abstain from using computer attacks and investigate public and private actors that conduct such attacks against civil society and media organizations.

Respect and guarantee the right to privacy of communications as established in the Organic Telecommunications Law. The right to privacy is a right in and of itself and is fundamental to the exercise of the right to freedom of expression.

Promote effective universal internet access in Venezuela, with stable, reliable connections that are high quality enough to allow for full inclusion of Venezuelans, facilitating the exercise of human rights and economic and social development.

Publish data and statistics on internet access, speed, and connection quality early, particularly in at-risk communities and rural areas.

Methodology

INTERNET BLOCKS

We use OONI Probe, the Open Observatory of Network Interference (OONI) network measurement software, to measure internet censorship in Venezuela. The probe is performed several times a day from various points of access in the Venezuelan network. OONI Probe is free, open software, and is specially designed to detect different times of online interference.

The main OONI tests used in this report (though they have others) are:

WEB CONNECTIVITY

TOR

WHATSAPP

BRIDGE REACHABILITY

FACEBOOK MESSENGER

TELEGRAM

The OONI web connectivity test is designed to measure whether websites are blocked using DNS manipulation, a TCP/IP block or a transparent proxy. This test is automatically conducted regarding the user perspective and uncensored control perspective. If the results of the two perspectives match, the most likely scenario is that the website tested can be accessed. However, if the results differ, the measurement is marked as anomalous.

We also conduct additional network measurement tests using dedicated equipment.

In order to monitor access to popular instant messaging platforms over time, we conducted OONI tests of WhatsApp, Facebook Messenger, and Telegram. These tests are designed to measure the accessibility of applications and web interfaces through DNS searches and attempts to establish TCP connections at their end points.

In light of the increase in censorship events over the past few years, we also decided to monitor access to censorship avoidance tools. Many avoidance tool sites are included on the Citizen Lab global testing list, which we measure by testing OONI web connectivity. We also conducted accessibility tests of the OONI Tor bridge, which is designed to measure Tor network and Tor bridge blocks.

Connectivity

The technical analysis of connectivity levels in real time is based on data generated by Internet Outage Detection and Analysis (IODA). Using its own data source, it generates a global history of connectivity data that covers various indicators.

Those data are processed and analyzed to identify national drops in connectivity. The entity also investigates the origin of such drops.

A drop in connectivity is defined as an incident that influences each state of the country differently. As such, it is defined as a regional drop event or drop in a specific ISP caused by a specific incident.

Two data classification categories were identified for the criteria for identifying the incidents/events:

Magnitude of the drop of connectivity levels:

CRITICAL

SERIOUS

MILD

Critical: 0-50%

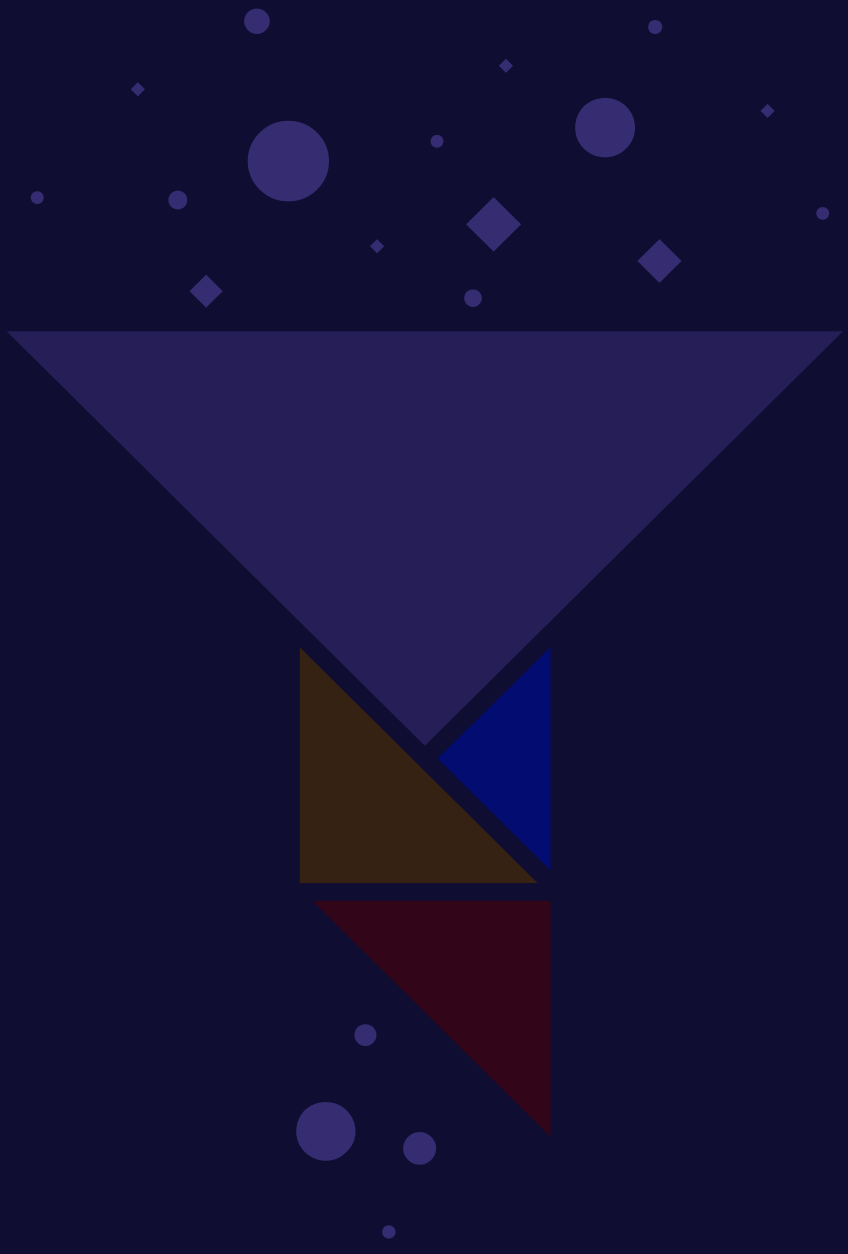
Serious: 51-80%

Mild: If the drop is not lower than 80% and also coincides with a clear connectivity drop event.

Cause of the incident:

It is important to note that the measurements use /24 normalized network segments compared to the highest connectivity value in the region or ISP that is being monitored as a metric.

The main purpose of this process is to identify major connectivity drops (macrosopic) that have a significant impact on the country and/or region and/or an ISP in Venezuela.



Caracas, abril 2022