Informe sobre situación de los derechos humanos digitales en Venezuela

SIN RESPIROS EN #INTERNETVE

REPORTE

2022 - 2023H1

CENSURA
BLOQUEOS
VIGILANCIA
CONECTIVIDAD
ATAQUES DIGITALES

VESINFILTRO.COM

VE SIN FILTRO

ACCESO A INTERNET EN VENEZUELA..... 2
Rendimiento de las conexiones a internet..... 4
Penetración de Internet..... 5
Velocidad de Internet..... 9
Oferta..... 11
Costo..... 11
Distribución Geográfica..... 12
EVENTOS DE CENSURA..... 13
Medios de Comunicación..... 14
Activistas DDHH..... 16
Contenido Para Adultos..... 17
Herramientas de evasión y sus riesgos..... 18
1er semestre 2023..... 19
CONECTIVIDAD Y DISPONIBILIDAD DEL SERVICIO DE INTERNET..... 19
Incidentes De Conectividad..... 20
Según El Tipo De Falla..... 24
Según La Duración Del Incidente Y Los Eventos..... 26
Duración De Los Incidentes Críticos Y Serios..... 27
Incidentes por falla de Isp y según la magnitud..... 28
Duración De Falla Por Isp..... 30
1er semestre 2023..... 32
PROTECCIÓN DE DATOS PERSONALES Y SEGURIDAD DE SITIOS WEB DEL ESTADO..... 33
SEGURIDAD Y CONFIANZA DE SITIOS WEB DEL ESTADO..... 34
FALTA DE ACCESIBILIDAD COMO LIMITACIÓN AL EJERCICIO DE DERECHOS EN INTERNET..... 36
Limitaciones a personas con discapacidad..... 36
AMENAZAS A LA PRIVACIDAD..... 38
Monitoreo de redes social..... 39
Espionaje e interceptación a las telecomunicaciones..... 40
Videovigilancia..... 42
EXTRACCIÓN DE DATOS, BORRADO Y REVISIÓN DE EQUIPOS BAJO COERCIÓN..... 43
ATAQUES DIGITALES..... 44
PHISHING Y ROBO DE CUENTAS..... 44
Ataques y hackeo a servidores..... 45

ACCESO A INTERNET EN VENEZUELA

El acceso a Internet es considerado un derecho humano por la Organización de las Naciones Unidas y permite a las personas ejercer su derecho a la libertad de expresión, acceder a la información y participar en actividades sociales y económicas.

En 2015, Naciones Unidas estableció los Objetivos de Desarrollo Sostenible (ODS), de los cuales la meta 9c es "aumentar significativamente el acceso a Internet y a las tecnologías de la comunicación (TIC) y esforzarse por proporcionar acceso universal y asequible a Internet en los países menos adelantados para 2020".

La mejora del acceso a Internet también puede contribuir a la consecución de otros ODS, como la reducción de la pobreza, el fomento del crecimiento económico y la mejora de la educación y la sanidad. El Programa de las Naciones Unidas para el Desarrollo (PNUD) creó el Índice de Pobreza Multidimensional (IPM), en el que el acceso a internet es uno de sus cinco aspectos claves.

La Unión Internacional de Telecomunicaciones (UIT) estimó que un aumento del 10 por ciento en la penetración de la banda ancha fija podría suponer un incremento del 1,57% en el producto interno bruto regional de América Latina y el Caribe.

La conectividad a Internet se correlaciona positivamente con una mayor participación en la población activa, la movilidad laboral, la creación de empleo y su crecimiento general. El acceso a Internet también refuerza la resiliencia económica y social al facilitar el acceso a servicios públicos esenciales como la educación y la atención médica, así como a oportunidades de formación y trabajo a distancia.

Venezuela pasó de tener un ecosistema de telecomunicaciones competitivo y vibrante, en comparación con sus pares, a tener uno de los peores servicios de Internet del mundo, que apenas comienza a mejorar pero de manera muy desigual, con las clases sociales más pudientes obteniendo un servicio de mayor calidad y los menos afortunados estancados en un acceso básico. El potencial acceso generalizado a Internet se ha visto frustrado por las crisis económica y política que han afectado negativamente al desarrollo de un acceso a Internet significativo. Cabe destacar el Decreto Presidencial de 2020 sobre "Eliminación del Gasto suntuario y superfluo" que, como política, catalogaba el acceso a Internet como un lujo.

Las fuentes de información que cubren el acceso a Internet en Venezuela tienden a ofrecer cifras diferentes debido a las distintas metodologías. Por ejemplo, CONATEL, el organismo nacional regulador de las telecomunicaciones, no ofrece públicamente detalles sobre sus metodologías, pero tiene datos de todos los proveedores de internet y abonados al servicio, y publica métricas desactualizadas, como se desprende de los rangos de fechas incluidos en sus informes.

El acceso libre, transparente y equitativo a datos e información de interés público es esencial para el análisis de los factores que configuran Internet en Venezuela, pero el acceso a la información pública está severamente restringido y las instituciones suelen ignorar las solicitudes de información. La evaluación de

Transparencia Venezuela sobre la Ley de Transparencia y Acceso a la Información de Interés Público de 2021 es que, lejos de garantizar ese derecho, consolidó aún más el secretismo.

Las medidas de control adoptadas en Venezuela desde 2020 para limitar la propagación del COVID-19 como resultado de la migración acelerada de las actividades laborales, educativas, económicas y sociales a la esfera digital, crearon presiones adicionales sobre la infraestructura de Internet en el país y aumentaron la necesidad de servicios de Internet de mayor calidad.

Las restricciones generalizadas a la libertad de prensa, incluidas la censura y la autocensura, obligan a los medios tradicionales, como los periódicos y las emisoras de radio y televisión, a abandonar los mercados analógicos.

Del mismo modo, al desaparecer prácticamente los periódicos independientes, desaparecer las opiniones críticas y las noticias de la televisión, proliferar la censura y disminuir el número de emisoras de radio independientes, muchos ciudadanos han recurrido a Internet para mantenerse informados. El acceso a Internet se ha convertido así en esencial para el ejercicio de los derechos políticos y civiles, a pesar de las restricciones impuestas por el régimen de Nicolás Maduro.

La compleja crisis humanitaria de Venezuela hace a menudo necesario el acceso a Internet para quienes buscan información sobre la disponibilidad de productos o servicios escasos. Estas situaciones suponen un riesgo para su seguridad física, sus condiciones y oportunidades migratorias y la posibilidad de acceder a servicios y ayudas públicas.

Rendimiento de las conexiones a internet

La mala calidad de Internet puede tener efectos negativos sobre las condiciones sociales en Venezuela, en particular para los miembros de poblaciones vulnerables como los niños, las mujeres, las minorías (migrantes, indígenas y otros) y las personas de bajos ingresos. Los venezolanos se enfrentan diariamente a múltiples retos que pueden verse agravados por la falta de acceso a tecnologías y servicios digitales de alta calidad.

Algunos aspectos técnicos relacionados con la calidad que pueden tener un impacto crítico en las actividades que se pueden completar en línea incluyen:

Velocidad: es uno de los aspectos más críticos de la calidad de Internet, incluyendo tanto la velocidad de descarga como la de subida. La velocidad de descarga se refiere a la velocidad a la que los datos se transfieren de Internet a un dispositivo, como cuando se descargan imágenes; la velocidad de subida es a la que los datos se transfieren de un dispositivo a Internet, como cuando se publica una foto en las redes sociales. La velocidad de Internet, también llamada ancho de banda, se divide entre los usuarios de una red. Algunas actividades, como el streaming de videos o música, requieren velocidades más altas que otras, como leer un artículo en línea.

Latencia: se refiere al tiempo que tardan los datos en viajar de un punto a otro de una red. Suele medirse en milisegundos. Una latencia más baja significa tiempos de respuesta más rápidos y una mejor

experiencia, especialmente para aplicaciones interactivas y en tiempo real; una latencia más alta puede imposibilitar muchas tareas, especialmente las videoconferencias. Incluso las reuniones sólo de voz pueden ser imposibles en redes con altos niveles de latencia.

Pérdida de paquetes: se produce cuando partes de la comunicación no llegan a su destino mientras se transmiten por una red. Una pérdida de paquetes elevada puede dar lugar a una experiencia de usuario deficiente, como audio o video entrecortados y retrasos o falta de información.

En este contexto, los niños y jóvenes pierden oportunidades educativas y de aprendizaje de calidad cuando sólo tienen acceso a conexiones de mala calidad.

Del mismo modo, las personas con bajos ingresos pueden tener dificultades para satisfacer sus necesidades básicas o acceder a programas de protección social por falta de acceso a las plataformas en línea, los pagos digitales o los sistemas de identificación necesarios. También pueden quedarse atrás en términos de generación de ingresos u oportunidades de empleo debido a la falta de alfabetización digital o de recursos digitales.

Penetración de Internet

Para el primer trimestre del año 2022 la Comisión Nacional de Telecomunicaciones (CONATEL) estimó que la penetración de internet en 55,34% a nivel nacional, son sus cifras más actualizadas. Para el cierre de 2020 fue de 53,66%, mientras que para inicios del 2021 hubo un aumento de 6,61 puntos porcentuales, luego en el 2do trimestre de 2021, hubo un descenso de 1,66 puntos porcentuales, el tercer trimestre se alcanzó una penetración de 62,25%, siendo esta la cifra más alta registrada entre finales del 2020 e inicios del 2022, después en el último trimestre de 2021 se presentó un descenso de 8,2 puntos porcentuales, y finalmente para inicios de 2022 hubo un leve descenso de 0,35 puntos porcentuales, teniendo así la cifra de penetración del primer trimestre del año 2022 (53,7%), finalmente se publicó que para el último trimestre del 2022 hubo un aumento en la penetración en comparación con el primer trimestre de 1,64 puntos porcentuales. Las cifras de penetración del 2do y 3er trimestre de 2022 no fueron publicadas por CONATEL, por lo que se realizó una estimación de estos datos.

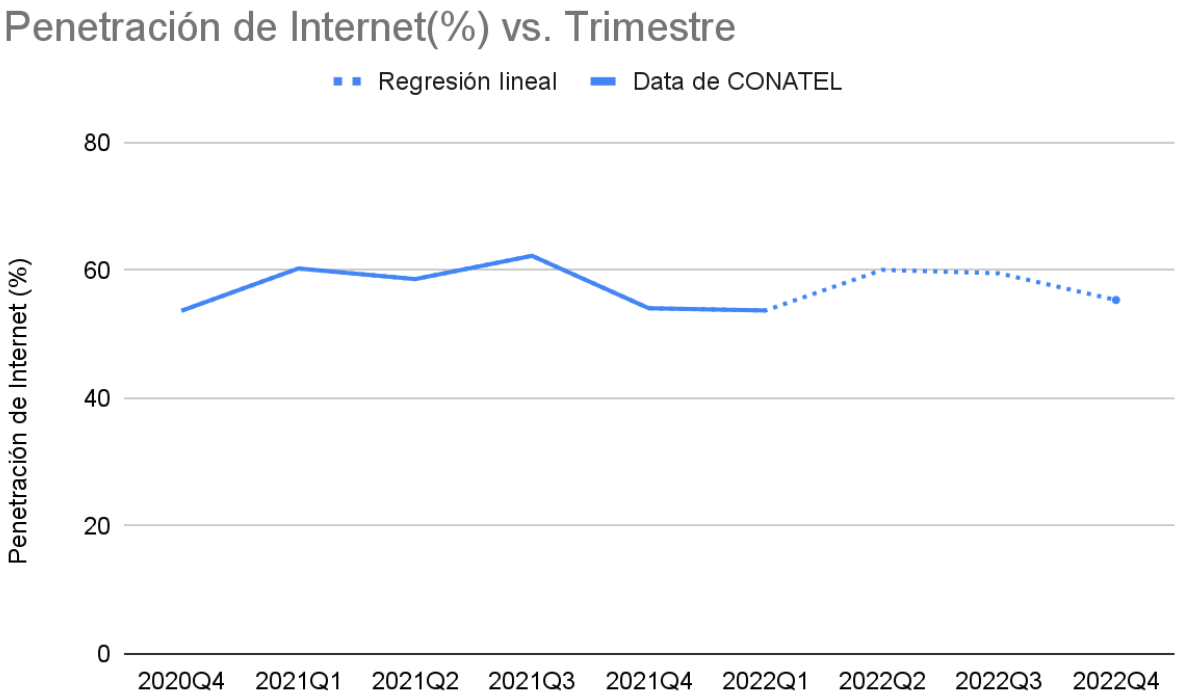


Gráfico de la penetración de Internet en Venezuela por trimestre anual, determinada utilizando las cifras de penetración de Internet de CONATEL. El 2do y 3er trimestre de 2022 fueron datos estimados porque los datos no se encuentran publicados . (Fuente: VE sin Filtro vía CONATEL)

Las fuentes disponibles sobre penetración de Internet en Venezuela suelen diferir por importantes márgenes usando diferentes metodologías. El Observatorio Venezolano de Servicios Públicos, en Mayo del año 2022, estimó que el 42,8% de la población tenía servicio de internet fijo[1], evidenciando un aumento de 8,6 puntos porcentuales entre enero de 2021 y mayo de 2022, mientras que 87.5% contaba con el servicio de internet móvil en mayo de 2022, lo que significa un aumento de 14.5 puntos porcentuales desde enero de 2021.

Considerando el acceso a datos de proveedores de internet y la dificultad de estas estimaciones, podemos utilizar las cifras de CONATEL como referencia principal; así mismo podemos estimar que la variación de la penetración de internet durante los últimos 3 trimestres de 2022 fue de un aumento de entre 6 y 15 puntos porcentuales, tomando los valores extremos de cambio reflejado por otras fuentes con datos más actualizados.

Según los índices de penetración publicados por Kepios en sus primeros informes de 2023, Venezuela tiene una de las tasas de penetración de Internet más bajas de América Latina, ubicándose en el quinto lugar. Esta tasa es inferior a la media de América Latina y el Caribe, que es del 76,64%. El aumento de la penetración de Internet es crucial para el desarrollo económico y la inclusión social. Investigaciones han

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

demostrado que el aumento del acceso a internet de banda ancha tiene un impacto positivo en las tasas de crecimiento económico.

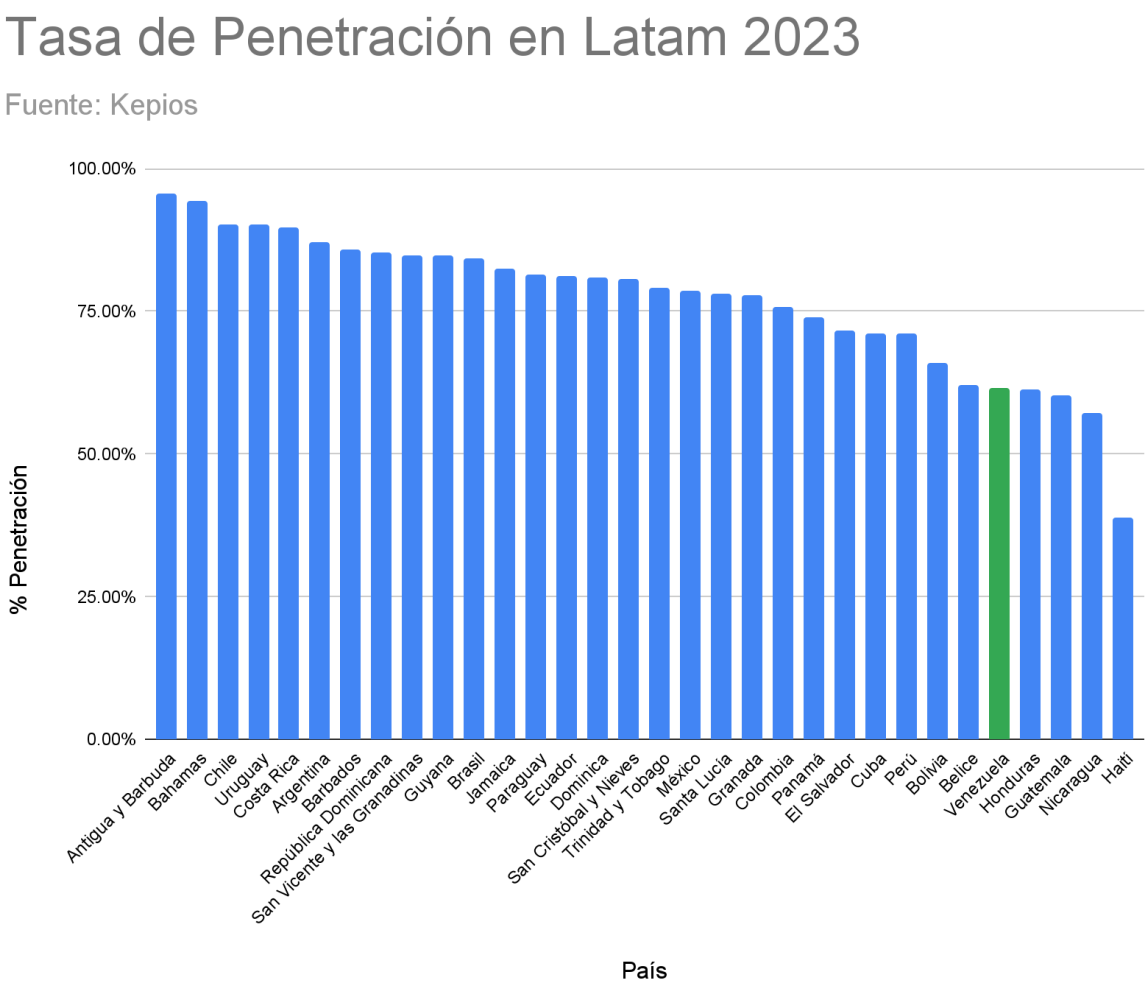


Gráfico de barras que muestra la tasa de penetración en América Latina basada en datos de Kepios de su primera publicación del año 2023. (Fuente: VE sin Filtro, utilizando datos de Kepios).

Con respecto a la distribución de los usuarios, el reporte de CONATEL correspondiente al primer trimestre del año 2022, evidencia la desigualdad en el acceso a Internet en el país, los 10 estados con menor penetración (de menor a mayor) son Amazonas, Delta Amacuro, Apure, Sucre, Yaracuy, Guárico, Falcón, Trujillo, Monagas y Portuguesa. Para el último trimestre los estados Falcón y Monagas cambiaron de posición y la penetración del estado Cojedes decae por lo que ocupa el último puesto de esta lista, mientras que los estados Distrito Capital y Miranda, que corresponden a la zona capital, tienen 167,34% y 90,22% de penetración de internet respectivamente. Para finales de año, Distrito Capital y Miranda continuaron siendo los estados con mayor penetración, pero Distrito Capital aumentó 30,36 puntos porcentuales, por el contrario Miranda disminuyó 2,24 puntos. La metodología indefinida de CONATEL para estimar el número de usuarios del servicio de Internet podría influir en la estimación de la penetración

del Distrito Capital (167,34%), otra posible razón podría ser que los datos se hayan recogido incorrectamente debido a la confusión en torno a los límites políticos en Caracas, entre el Distrito Capital, el Distrito Metropolitano de Caracas y el estado Miranda.

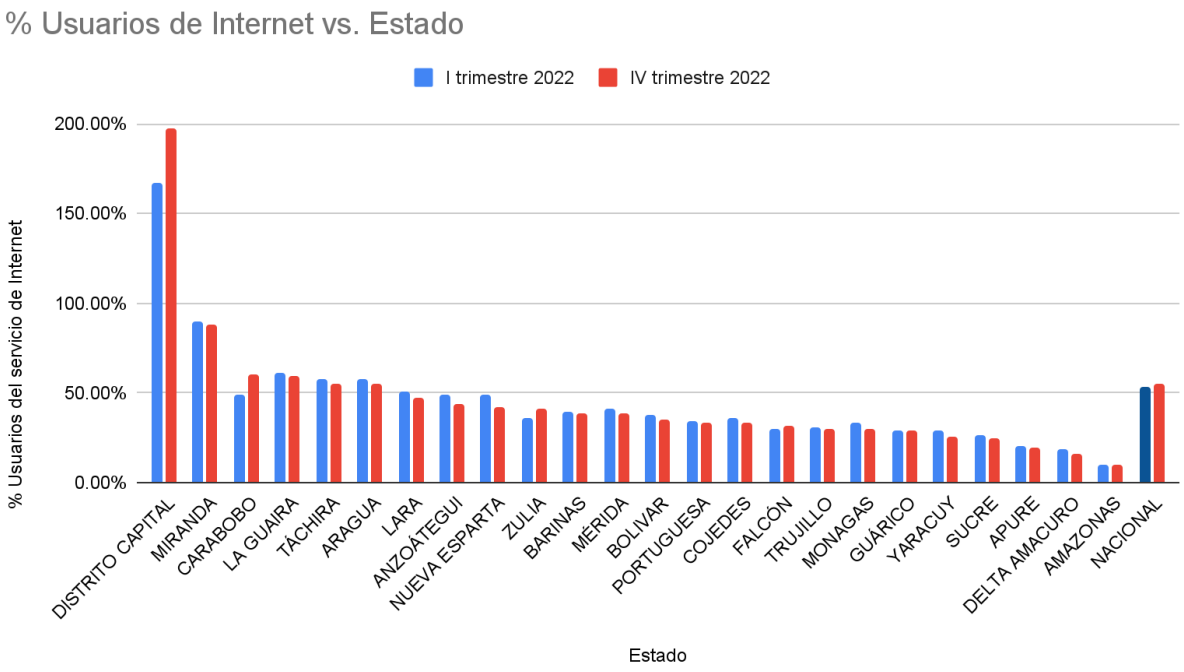


Gráfico de barras del porcentaje de usuarios del servicio de Internet por estado de Venezuela para el 1er y 4to trimestre del año 2022. (Fuente: VE sin Filtro, utilizando datos de CONATEL)

Esto evidencia que hay una brecha digital entre los estados rurales y urbanos en el país. Los estados con mayores índices de penetración tienen una mayor densidad de población. 22 de los 24 estados de Venezuela tienen un acceso a Internet inestable y desigual, lo que se correlaciona positivamente con la densidad de población del país.

Las cifras oficiales de penetración de Internet asumen que todos los clientes de servicios de Internet tienen una conexión en funcionamiento, pero un gran número de clientes de CANTV, el proveedor de servicios de Internet (ISP) con mayor alcance geográfico, no han tenido servicio durante meses o años. Según el Observatorio Venezolano de Servicios Públicos (OVSP), el 41,2% de los venezolanos sin acceso a Internet afirman que la razón es la falta de servicio de CANTV. No está claro si los encuestados incluyeron lugares sin cobertura y aquellos cuyo servicio no funcionaba.

Un suceso que demostró las consecuencias del acceso limitado a Internet para la seguridad física y el derecho a la vida fue un enfrentamiento en el municipio de Alto Orinoco, en el estado de Amazonas, ocurrido el 20 de marzo de 2022, entre militares venezolanos y miembros de un grupo indígena. En el altercado, los soldados venezolanos abrieron fuego contra un grupo de yanomamis después de que éstos les pidieran que compartieran el acceso a su servicio de Internet, dejando cuatro muertos (una mujer y tres hombres) y otros cinco heridos (entre ellos un joven de 16 años).

Velocidad de Internet

La velocidad de Internet puede suponer un obstáculo para su uso y puede verse afectada por múltiples factores. Hay varias formas de medir la velocidad de Internet, y no siempre son comparables. Algunas fuentes importantes, como la empresa de pruebas de redes Ookla, pueden presentar sesgos, ya que no utilizan una muestra aleatoria de conexiones de todo el país; en su lugar, utilizan información voluntaria de personas, a menudo más expertas en tecnología, que, por ejemplo, pueden proporcionar mediciones de velocidad utilizando la herramienta de Ookla para determinar la velocidad de su conexión.

En Venezuela, la velocidad media de Internet fija es de 16,5 Mbps para descarga, la segunda más lenta de América Latina. Se sitúa por detrás de Cuba, con 1,84 Mbps para descarga según el Índice Global Speedtest de la empresa de pruebas de redes Ookla (a enero de 2023). En el extremo opuesto, Chile tiene la velocidad media de descarga más alta de la región (224,84 Mbps) y la segunda más rápida del mundo. Del mismo modo, la velocidad media de subida de Venezuela, de 13,33 Mbps, es diez veces más lenta que la de Chile (133,81 Mbps). Venezuela ocupa el puesto 138 de los 179 países incluidos en la muestra de Ookla.

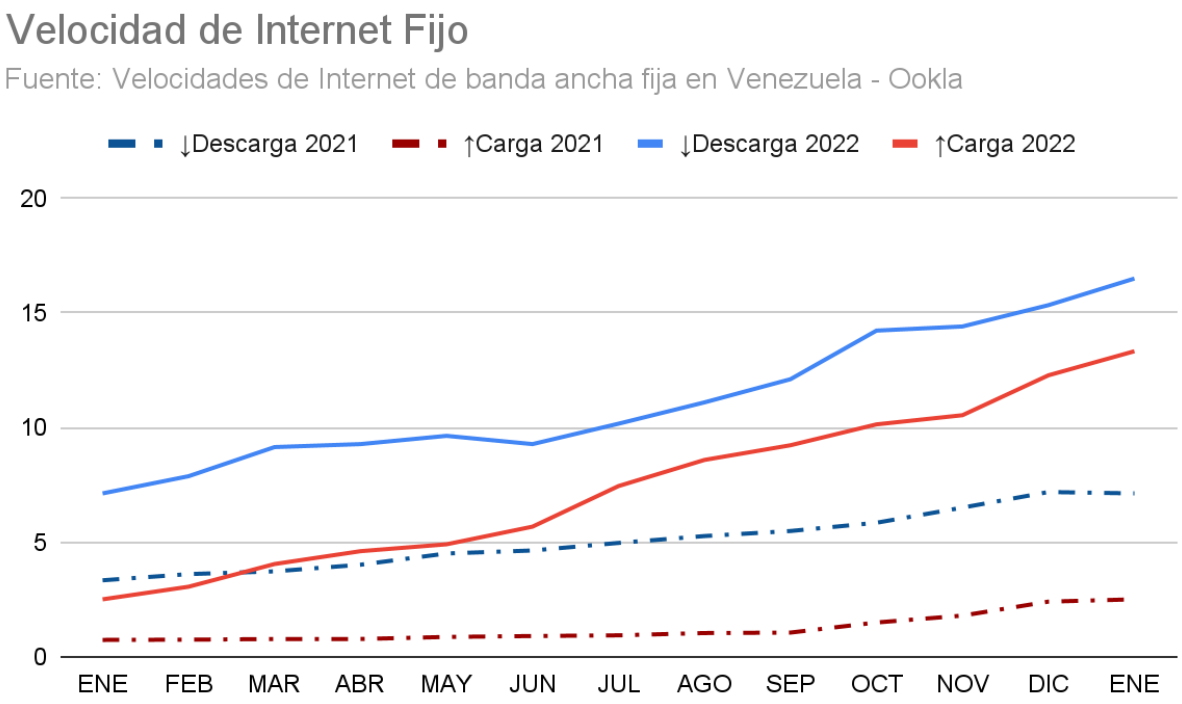


Gráfico de Velocidad de Internet banda ancha fija de carga y descarga del año 2021 y 2022. (Fuente: VE sin Filtro, utilizando datos de Ookla).

Comparando con las cifras de OOKLA de 2022, la velocidad mediana de descarga durante enero de 2022 fue 7,13 Mbps, lo que significa que hubo un aumento del 131,4%. La de subida fue de 2,51 Mbps (Enero 2022), en este caso el aumento experimentado durante el 2022 fue de 431,1%.

M-Lab, un proyecto con colaboradores de la sociedad civil, instituciones educativas y el sector privado, utiliza una metodología diferente que se centra en la velocidad de un único hilo de comunicación entre tu dispositivo y un servidor. Esto es más preciso para la calidad del efecto de la red en aplicaciones individuales, mientras que el enfoque multi hilo que viene por defecto en la prueba de velocidad de Ookla es más preciso para el ancho de banda máximo cuando está saturado por múltiples aplicaciones o aplicaciones multihilo como el streaming de vídeo. También hay sesgos de selección introducidos por la fuente de las mediciones individuales en cada uno.

M-lab coloca la velocidad mediana de Internet en Venezuela entre 1,02 y 5,21 Mbps de descarga y entre 1,63 y 4,29 Mbps de carga, durante enero de 2022 y enero de 2023, usando su prueba de un solo hilo de tráfico. La metodología de M-Lab representa mejor el desempeño de la conexión para tareas demandantes individuales, pero las cifras de velocidad resultan inferiores a lo que se esperaría en muchos casos reales, donde hay múltiples descargas en simultáneo.

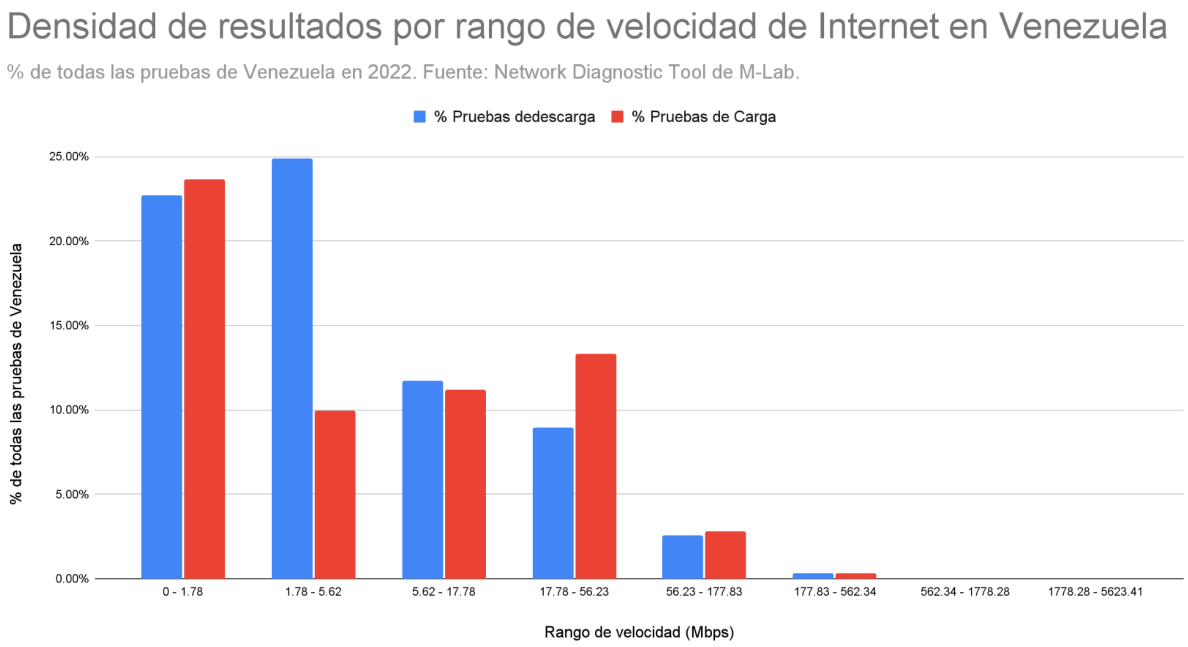


Gráfico de barras de la distribución de los resultados de las pruebas de velocidad en Venezuela por rango de velocidad durante el año natural 2022 utilizando mediciones de Network Diagnostics Tool. (Fuente: VE sin Filtro, utilizando datos de M-Lab).

Las cifras de M-lab muestran claramente que el 22.7% y el 24.9% de las pruebas de velocidad de descarga se encuentran entre los rangos de 0 - 1,78 Mbps y 1,78 - 5,62 Mbps respectivamente, mientras que con respecto a los resultados de las pruebas de velocidad de carga el 23,6% se encuentra en el rango de 0 - 1,78 Mbps.

Según estas mediciones realizadas con la Herramienta de Diagnóstico de Redes de M-Lab, durante el 2022, al menos el 59% de los usuarios de Internet en Venezuela sigue teniendo conexiones de banda ancha insuficientes, lo que limita o impide a los usuarios desarrollar plenamente ciertas actividades. A pesar del reciente aumento de las velocidades medias, es importante tener en cuenta que la velocidad media es el punto en el que la mitad de los usuarios tiene una velocidad menor y el resto de la muestra

disfruta de velocidades de conexiones muy superiores. Esto significa que muchos usuarios de Internet con conexiones residenciales tienen problemas para acceder a los servicios necesarios y ejercer sus derechos en línea, por no hablar de las personas que no tienen acceso a Internet en su casa o dependen exclusivamente de Internet móvil a través de planes de telefonía celular de prepago.

Oferta

Las tecnologías actualmente disponibles en la oferta del mercado de ISP son líneas de suscriptor digital (DSL), cable coaxial, fibra óptica, radiofrecuencia y microondas.

Según el análisis realizado por VESinFiltro de la oferta del servicio de Internet para principios de 2023, el 60,53% son planes de fibra óptica, seguidos de radiofrecuencia (19,3%), cable coaxial (8,77), DSL (6,14) y microondas (5,26). La tecnología con mayor número de usuarios es la DSL, con 2,2 millones, seguida del módem por cable (210.000 usuarios), la fibra hasta el hogar/edificio (67.000), la conexión inalámbrica fija terrestre (10.000), otra banda ancha fija (2.000) y la banda ancha por satélite (25).

En cuanto a la demanda, según datos del último reporte de monitoreo del OVSP de diciembre de 2022, en el último cuatrimestre del año hubo entre un 54,5% y 57,2% de usuarios a nivel nacional con servicio de Internet por CANTV, 32,95% y 30,19% de usuarios con internet de fibra óptica por un proveedor privado, mientras que los usuario de Internet mediante un servicio “satelital” (radiofrecuencia o microonda) estuvieron entre 4,31% y 5,21%, en cuanto a los usuarios que no poseen servicio de Internet, registraron que es entre un 6,72% y 7,39%[2].

En cuanto a la velocidad de los planes disponibles, el 60,5% de los planes disponibles tienen velocidades iguales o superiores a 30 Mbps. De estos, el 84% se entrega utilizando fibra óptica y el resto utiliza radiofrecuencia o cable coaxial.

Los planes con velocidades inferiores a 30 Mbps utilizan principalmente tecnología DSL, radiofrecuencia, microondas o cable coaxial, mientras que todos los planes por encima de 100 Mbps utilizan fibra óptica.

Costo

Un análisis de los paquetes de servicios de 24 ISPs nacionales demuestra el elevado coste de los servicios, que es un obstáculo para el acceso a Internet de los venezolanos. La comparación entre el precio de 115 planes analizados y el salario mínimo presenta un rango amplio de precios, desde 0,08 hasta 56,22 veces el salario mínimo mensual, o desde 0,41 USD (para un pequeño plan de datos celulares por consumo) hasta 300 USD (para planes de fibra óptica con velocidad de 1Gbps).

En este rango de precios, la distribución de los planes disponibles no es uniforme. Hay 26 planes disponibles que cuestan entre 4,44 y 6,93 veces el salario mínimo mensual, lo que representa el 22,6% de

2 https://www.monitoreocomunitario.org/_files/ugd/eca97a_4135911246a24be5afe0e4add066af54.pdf

los planes analizados. Y el 70,4% (81 planes) de los planes ofertados tienen precios entre 4,44 y 56,22 veces el salario mínimo mensual. El precio medio de los paquetes de Internet revisados fue de 6,93 veces el salario mínimo mensual; aunque esto no refleja los gastos medios en acceso a Internet, muestra cómo gran parte del mercado se centra en la gama alta, dejando pocas opciones asequibles para quienes se encuentran en el salario mínimo mensual o justo por encima de él.

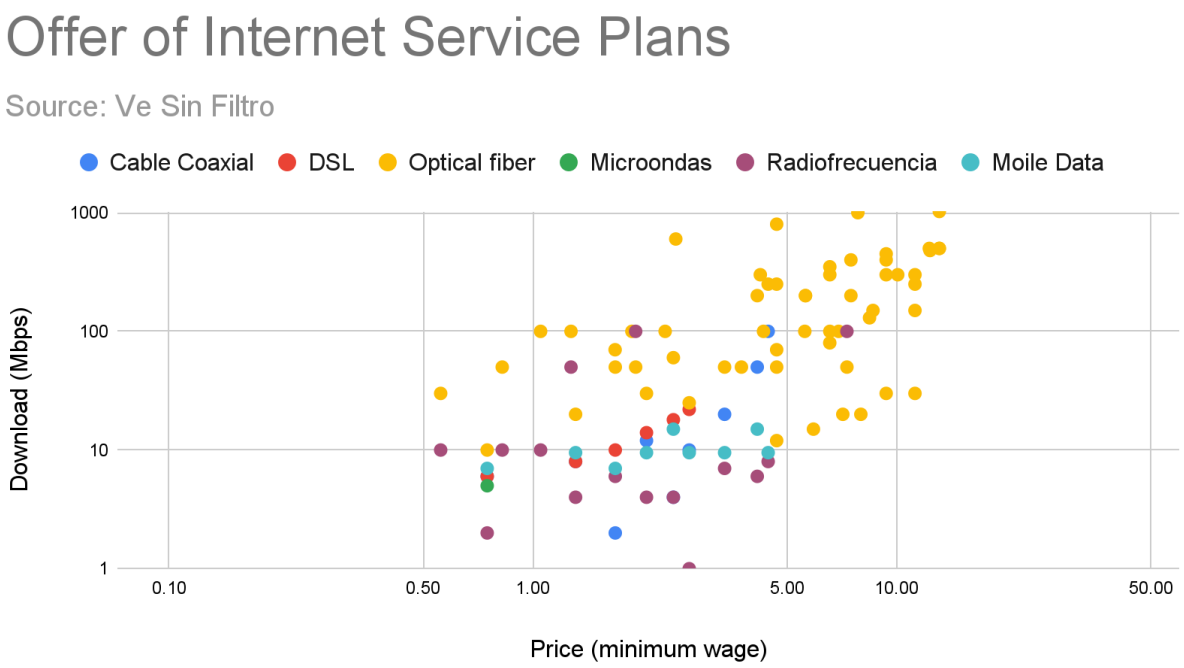


Gráfico de dispersión de los planes de servicio de Internet en Venezuela por velocidad de descarga y precio en función del salario mínimo mensual venezolano de 2022. (Fuente: VE sin Filtro)

Es importante tener en cuenta que la inflación que ha experimentado Venezuela en los últimos años ha disminuido significativamente el poder adquisitivo de una gran mayoría de venezolanos. El hecho de que sólo el 13,27% de los planes de servicio de Internet tengan precios inferiores a un salario mínimo mensual es preocupante en el sentido de que la falta de opciones asequibles de alta calidad presenta, junto con la falta de infraestructura general en zonas que llevan mucho tiempo sin servicio fiable o sin servicio en absoluto, una de las mayores barreras para el acceso significativo a Internet. Diez de estos trece planes son planes de datos móviles con límites de uso de datos que oscilan entre 50 MB y 10 GB al mes.

Distribución Geográfica

En cuanto a distribución geográfica de la oferta del servicio de internet, es relevante la desigual distribución en los distintos estados y otros territorios del país: mientras que la mitad de los ISP ofrecen servicios en Caracas, la mayoría de los lugares no tienen muchas opciones, si es que tienen alguna. Miranda tiene el segundo nivel de servicio más alto, con ocho ISP, seguido de Zulia (seis) y Carabobo (cinco). Existe una alta correlación positiva con la densidad de población, ya que los estados con ofertas

más limitadas son también los que tienen bajos índices de penetración, a saber, Amazonas, Anzoátegui, Apure, Cojedes, Guárico, Mérida, Portuguesa, Sucre, Táchira, Yaracuy y Delta Amacuro.

En algunos estados fronterizos, los ISP se aprovechan de la proximidad de la frontera y algunos ciudadanos utilizan servicios inalámbricos del país vecino para acceder a Internet. El periodista especializado en telecomunicaciones William Peña afirmó que algunos ISP contratan a proveedores de países fronterizos para reducir costos y ofrecer mejor ancho de banda o precios más bajos, como los que se ofrecen en Zulia que se conectan a Internet a través de proveedores colombianos.

El presidente de Casatel, Pedro Marín, explicó que una de las razones por las que la mayoría de los ISP dan servicio sólo a unas pocas ciudades importantes, principalmente Caracas, Maracaibo, Barquisimeto y Valencia, es el alto coste de utilizar las "Vías Generales de Telecomunicaciones", una parte común de la infraestructura física utilizada por las redes de telecomunicaciones que es propiedad y está gestionada por empresas estatales en Venezuela.

EVENTOS DE CENSURA

En Venezuela, el acceso a la información es crucial debido a la compleja dinámica social que experimenta el país. La censura en los medios tradicionales y el crecimiento global de Internet hacen que el acceso a la red sea esencial para los derechos civiles y políticos.

El gobierno Venezolano bloquea sitios web como táctica de censura. Se identificaron bloqueos de varios tipos: DNS, HTTP/HTTPS y TCP/IP. Los ISP privados usan bloqueos DNS y CANTV emplea bloqueos HTTP/HTTPS y DNS. Cada bloqueo afecta las conexiones de los usuarios de manera diferente, y las VPN son necesarias para acceder a sitios bloqueados.

La mayoría de los bloqueos se basan en DNS. Los ISP reconfiguran servidores DNS para responder incorrectamente a las solicitudes de sitios web que desean bloquear.

Los bloqueos HTTP y HTTPS examinan comunicaciones en busca de elementos específicos, lo que requiere herramientas como VPN para evadir la censura.

Más de cien URLs están bloqueadas en Venezuela, incluyendo sitios independientes de noticias. Esto limita la libertad de expresión y el acceso a la información.

Categoría	Abreviatura	Casos de sitios web bloqueados	URLs o dominios bloqueados	Total de eventos de bloqueo
E-commerce	COMM	1	3	19
Economics	ECON	2	4	21
Hate Speech	HATE	0	1	6
Human Rights Issues	HUMR	3	3	14
Media Sharing	MMED	3	3	14

News Media	NEWS	47	66	314
Political Criticism	POLR	10	11	52
Pornography	PORN	2	2	2
Public Health	PUBH	2	2	8
Anonymization and circumvention tools	ANON	3	5	22
Total		**71**	**100**	**472**

Tabla que muestra el número de sitios web bloqueados por categoría (comercio electrónico, economía, incitación al odio, derechos humanos, intercambio de medios, medios de noticias, comentarios políticos, pornografía, salud pública y herramientas de anonimización y elusión), junto con su número total de sitios web bloqueados, sus URL bloqueadas y el total de eventos (incluidos los diferentes bloqueos aplicados o reaplicados por cada ISP) activos en 2022. (Fuente: VE sin Filtro)

Los bloqueos se extienden más allá de los medios informativos; en particular, esta censura se aplica también contra sitios dedicados a comentarios políticos y a sitios con contenido de derechos humanos. Todos los principales ISP examinados aplican bloqueos de Internet, incluyendo tanto entidades públicas como privadas: CANTV, Movistar, Inter, Digitel, Net Uno y Supercable.

Los bloqueos no sólo afectan a la libertad de información de los ciudadanos en Venezuela, sino que también son un obstáculo a la educación y al acceso a información de calidad para estudiantes e investigadores, así como al derecho a la libertad de asociación y el desarrollo de actividades laborales entre muchas otras.

Los bloqueos unilaterales de sitios web no se ajustan a las normas internacionales de derechos humanos. Se ordenan de oficio, a discreción del organismo regulador de las telecomunicaciones CONATEL, con total opacidad y sin una base jurídica clara. Estas órdenes de bloqueo de Internet se ejecutan sin garantías para el debido proceso y nunca son supervisadas o dictadas por un juez.

Medios de Comunicación

SITIO	DOMINIO	CATEGORIA	CANTV AS8048	Movistar AS6306	Digitel AS27717 AS264731	Inter AS21826	NetUno AS11562	SuperCable AS22313
6to poder	6topoder.com	NEWS	DNS	DNS	DNS	DNS	DNS	DNS
Alek boyd	alekboyd.blogspot.co.uk	NEWS	HTTP+DNS	DNS	DNS	No	DNS	
analisis 24	analisis24.com	NEWS	No	DNS	No	DNS	DNS	No
Antena 3	antena3internacional.com	NEWS	HTTP+DNS	No	No	No	No	No
dolar today	bit.ly	NEWS	No	HTTP	No	No	No	
Dolar Paralelo	dolarparalelo.biz	NEWS	HTTP+DNS	No	DNS	No	DNS	No
Dolar Paralelo	dolarparalelovenezuela.com	NEWS	HTTP+DNS	No	DNS	No	DNS	No
Dolar Paralelo	dollarparalelovenezuela.com	NEWS	HTTP+DNS	DNS	DNS	No	DNS	DNS
eldolarparalelo.info	eldolarparalelo.info	NEWS	HTTP+DNS	DNS	DNS	DNS	DNS	DNS
El Pitazo	elpitazo.info	NEWS	HTTP+DNS	DNS	DNS	No	DNS	

SITIO	DOMINIO	CATEGORIA	CANTV AS8048	Movistar AS6306	Digitel AS27717 AS264731	Inter AS21826	NetUno AS11562	SuperCable AS22313
El Liberal Venezolano	liberal-venezolano.blogspot.com	NEWS	HTTP+DNS	DNS	DNS	DNS	DNS	
noticias venezuela	noticiasvenezuela.org	NEWS	HTTP+DNS	DNS	DNS	DNS	DNS	
Sumarium	sumarium.es	NEWS	HTTP+DNS	No	No	No	No	
2001	www.2001.com.ve	NEWS	HTTP+DNS	No	No	No	No	No
Aguacate verde	www.aguacateverde.com	NEWS	HTTP+DNS	DNS	DNS	No	DNS	DNS
Infobae	www.infobae.media	NEWS	HTTP+DNS	DNS	DNS	DNS	DNS	DNS
Alberto News	albertonews.com	NEWS	HTTP+DNS	DNS	DNS	DNS	DNS	
Alek boyd	alekboyd.blogspot.com	NEWS	No	DNS	DNS	No	DNS	
Al navio	alnavio.com	NEWS	HTTP+DNS	DNS	DNS	DNS	DNS	DNS
armando info	armando.info	NEWS	HTTP+DNS	DNS	DNS	DNS	No	DNS
Alberto News	awsveanews.com	NEWS	HTTP	No	No	No	No	
Alberto News	b1tly4n3s.com	NEWS	HTTP	No	No	No	No	
Caraota digital	caraotadigital.news	NEWS	HTTP+DNS	DNS	DNS	DNS	DNS	
Caraota digital	caraotadigital.xyz	NEWS	HTTP+DNS	DNS	DNS	DNS	DNS	
cronica.uno	cronica.uno	NEWS	HTTP+DNS	DNS	DNS	DNS	DNS	DNS
Diario La region	diariolaregion.net	NEWS	HTTP+DNS	DNS	No	DNS	DNS	
Dolar today	dolartoday.com	NEWS	HTTP	DNS	DNS	DNS	DNS	DNS
Dolar today	dolartoday.info	NEWS	HTTP+DNS	DNS	DNS	DNS	DNS	DNS
Dolar today	dolartoday.org	NEWS	HTTP+DNS	DNS	DNS	DNS	DNS	DNS
dollar.nu	dollar.nu	NEWS	HTTP+DNS	DNS	DNS	DNS	DNS	DNS
Efecto cocuyo	efectococuyo.com	NEWS	HTTP+DNS	DNS	DNS	DNS	DNS	
El diario	eldiario.com	NEWS	HTTP	No	No	No	No	No
El Pitazo	elpitazo.com	NEWS	HTTP+DNS	DNS	DNS	No	DNS	
El Pitazo	elpitazo.net	NEWS	HTTP+DNS	DNS	DNS	DNS	DNS	DNS
Insight Crime	es.insightcrime.org	NEWS	HTTP	No	No	No	No	No
EVTV	evtv.online	NEWS	HTTP+DNS	DNS	DNS	DNS	DNS	
EVTV	evtvmiami.com	NEWS	HTTP	DNS	DNS	DNS	DNS	
Infobae	infob.ae	NEWS	HTTP	DNS	DNS	HTTP	DNS	
La manada digital	lamananadigital.com	NEWS	HTTP+DNS	No	No	No	No	
La patilla	lapatilla.com	NEWS	HTTP+DNS	DNS	DNS	DNS	DNS	
Maduradas	maduradas.com	NEWS	HTTP+DNS	DNS	DNS	No	DNS	
Minuto 30	minuto30.com	NEWS	HTTP+DNS	DNS	DNS	DNS	DNS	DNS
Monitoreamos	monitoreamos.com	NEWS	HTTP	DNS	DNS	DNS	DNS	
noticia al dia	noticiaaldia.com	NEWS	HTTP+DNS	DNS	DNS	DNS	DNS	DNS
noticia al dia	noticialdia.com	NEWS	HTTP+DNS	DNS	No	DNS	DNS	

SITIO	DOMINIO	CATEGORIA	CANTV AS8048	Movistar AS6306	Digitel AS27717 AS264731	Inter AS21826	NetUno AS11562	SuperCable AS22313
primer informe	primerinforme.com	NEWS	HTTP+DNS	DNS	No	DNS	DNS	
Punto de corte	puntodecorte.com	NEWS	HTTP+DNS	DNS	DNS	DNS	DNS	DNS
Runrunes	runrun.es	NEWS	HTTP+DNS	No	No	No	DNS	No
Venezuela al dia	venezuelaaldia.com	NEWS	No	DNS	No	DNS	DNS	No
Vivo play	vivoplay.net	NEWS	No	DNS	DNS	No	DNS	No
VPITV	vpitv.com	NEWS	HTTP+DNS	No	DNS	DNS	DNS	
Caraota digital	www.adncaraota.com	NEWS	HTTP	No	No	No	No	
Aporrea	www.aporrea.org	NEWS	HTTP	No	No	No	No	
Alberto News	www.b1tlydns02io.com	NEWS	HTTP	No	No	No	No	
Caraota digital	www.caraotadigital.net	NEWS	HTTP+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 tiempo	www.eltiempo.com	NEWS	HTTP+DNS	DNS	DNS	DNS	DNS	
Infobae	www.infobae.com	NEWS	HTTP+DNS	DNS	DNS	DNS	DNS	DNS
Insight Crime	www.insightcrime.org	NEWS	HTTP	No	No	No	No	No
la patilla	www.lapatilla.com	NEWS	HTTP+DNS	DNS	DNS	DNS	DNS	DNS
noticiero digital	www.noticierodigital.com	NEWS	HTTP+DNS	No	No	No	No	No
ntn 24	www.ntn24.com	NEWS	HTTP+DNS	DNS	DNS	DNS	DNS	DNS
TV Venezuela	www.tvvenezuela.tv	NEWS	HTTP+DNS	DNS	DNS	DNS	DNS	
Venezuela al dia	www.venezuelaaldia.com	NEWS	No	DNS	DNS	DNS	DNS	DNS
VPITV	www.vpitv.com	NEWS	HTTP+DNS	DNS	DNS	DNS	DNS	DNS

Tabla que muestra los bloqueos activos de medios de comunicación, durante 2022, según lo registrado por VE sin Filtro. (Fuente: VE sin Filtro)

Activistas DDHH

Entre los diversos bloqueos impuestos por el Estado o los proveedores de servicios de Internet que cumplen las normas, VE sin Filtro ha constatado que en Venezuela se han bloqueado las páginas web de algunas ONG. Varias organizaciones han sido víctimas de bloqueos a lo largo de los años. Actualmente hay tres bloqueos activos de páginas de ONG en Venezuela.

SITIO	DOMINIO	CATEGORIA	CANTV AS8048	Movistar AS6306	Digitel AS27717 AS264731	Inter AS21826	NetUno AS11562	SuperCable AS22313
Mi Convive	miconvive.com	HUMR	HTTP+DNS	DNS	DNS	DNS	DNS	DNS
Change.org	www.change.org	HUMR	HTTP+DNS	DNS	DNS	DNS	DNS	
Justicia, Encuentro y Perdón	www.jepvenezuela.com	HUMR	HTTP	No	No	No	No	

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

VE sin Filtro determinó que el sitio web www.jepvenezuela.com, perteneciente a la ONG Justicia, Encuentro, y Perdón, se encuentra actualmente bloqueado. Esta organización ha monitoreado y manejado violaciones a los derechos humanos desde 2017, a menudo tomando acciones ante entidades nacionales e internacionales como un medio para asegurar justicia, protección y reparación para las víctimas de esas violaciones. La organización está llevando a cabo una campaña para conmemorar y exigir reparaciones para los venezolanos asesinados y detenidos en protestas entre 2014 y 2017. La ONG también informa sobre la tortura y el trato cruel e inhumano de los presos políticos en los centros de detención venezolanos. El 7 de junio de 2022, la organización denunció la detención arbitraria de jóvenes por parte de la policía municipal de Chacao, después de que participaran en una conmemoración pública de Neomar Lander, un joven de 17 años que se encontraba entre las 163 personas asesinadas durante el ciclo de protestas de 2017.

De acuerdo con las mediciones técnicas realizadas por VE sin Filtro, el sitio de la organización ha estado bloqueado para los clientes de CANTV desde al menos el 6 de junio de 2022, inicialmente como un bloqueo de tipo HTTP/HTTPS y actualmente seis eventos de bloqueo HTTP activos. VE sin Filtro también encontró que el ISP Movistar también mantiene un bloqueo HTTP.

Por otra parte, el 18 de mayo de 2020, el sitio web de Caracas Mi Convive, una ONG que promueve "la convivencia en Caracas a través de la organización comunitaria y la prevención de la violencia", fue bloqueado por los principales ISP de Venezuela. VE sin Filtro determinó que el bloqueo era de tipo DNS de los ISP CANTV, Movistar, Digitel, Inter, NetUno y Supercable. El bloqueo sigue activo en todos los ISP, aunque el tipo de bloqueo utilizado por CANTV es ahora tanto HTTP como DNS. Los otros ISPs tienen el mismo bloqueo DNS inicial, lo que significa que actualmente hay siete eventos de bloqueo activos para este dominio.

VE sin Filtro confirmó que la plataforma de incidencia Change.org fue bloqueada a través de CANTV el fin de semana del 22 de febrero de 2019, pocos días después de que varios medios de comunicación fueran bloqueados por cubrir la frontera de un evento en el que participaron Guaidó y el fundador de Virgin y filántropo Richard Branson. El evento, que pretendía movilizar apoyo y ofrecer ayuda humanitaria de forma pacífica, incluyó un concierto con artistas latinoamericanos. El motivo eran probablemente peticiones solicitando firmas en relación con el régimen de Maduro. Una pedía apoyo para una intervención militar, otra solicitaba la visita de la Alta Comisionada de las Naciones Unidas (ONU) para los Derechos Humanos, Michelle Bachelet.

Estos bloqueos impiden a los ciudadanos acceder a información clave y a herramientas de participación ciudadana. Por ejemplo, Change.org es una plataforma utilizada en todo el mundo para lanzar y recoger firmas para peticiones en línea que suelen dirigirse a políticos y poderosos para animarles a actuar. Por su parte, JEP Venezuela promueve el acceso a la justicia en el país, y Mi Convive trabaja en el ámbito de la seguridad ciudadana y la prevención de la violencia. Estos bloqueos también afectan a la capacidad de las organizaciones para realizar su trabajo y cumplir sus objetivos. Por lo tanto, el bloqueo del acceso a los sitios web de estas organizaciones constituye una violación del derecho a la libre asociación, así como un límite a la expresión.

Contenido Para Adultos

SITIO	DOMINIO	CATEGORIA	CANTV AS8048	Movistar AS6306	Digitel AS27717 AS264731	Inter AS21826	NetUno AS11562	SuperCable AS22313
Petardas	www.petardas.com	PORN	HTTP	No	No	No	No	No
HDZOG	hdzog.com	PORN	HTTP	No	No	No	No	No

Tabla que muestra los bloqueos activos de páginas de contenido para adultos, durante 2022, según lo registrado por VE sin Filtro. (Fuente: VE sin Filtro)

Herramientas de evasión y sus riesgos

El gobierno de Venezuela está bloqueando el acceso a las herramientas de evasión de la censura, como las VPN y Tor. Estos bloqueos están teniendo un impacto significativo en la capacidad de los venezolanos para acceder a información e interactuar con el contenido y la comunidad en Internet.

Los principales ISPs de Venezuela, incluidos CANTV, durante el 2022 continuaron bloqueando las páginas web de las VPN TunnelBear y Psiphon, desde el 2019 y el 2020 respectivamente. El bloqueo de TunnelBear es más completo, ya que afecta tanto a la página web como a la API de la aplicación, por parte de CANTV el bloqueo experimentado es de tipo de DNS además de HTTP/HTTPS simultáneamente desde 2019. Mientras que los demás proveedores mantienen activo el bloqueo de tipo DNS, desde el 20 de agosto de 2020. En el caso de Digitel hubo un levantamiento del bloqueo en 2021, entre el 7 de marzo y el 12 de octubre. El bloqueo de Psiphon afecta solo a la página web, pero los usuarios aún pueden acceder a la aplicación a través de URL alternativas.

CANTV también está intentando bloquear Tor, una herramienta de privacidad que se puede utilizar para evitar la censura. Los bloqueos de Tor están teniendo un impacto significativo en la capacidad de los venezolanos para acceder a información en línea que de otro modo estaría restringida.

SITIO	DOMINIO	CATEGORIA	CANTV AS8048	Movistar AS6306	Digitel AS27717 AS264731	Inter AS21826	NetUno AS11562	SuperCable AS22313
Psiphon	psiphon.ca	VPN	HTTP+DNS	DNS	No	DNS	DNS	DNS
Tunnel Bear	tunnelbear.com	VPN	HTTP+DNS	DNS	DNS	DNS	DNS	
API Tunnel Bear	api.tunnelbear.com	VPN	HTTP+DNS	DNS	No	No	DNS	DNS

Tabla que muestra los bloqueos activos de dominios de herramientas de evasión de censura, durante 2022, según lo registrado por VE sin Filtro. (Fuente: VE sin Filtro)

CANTV es el principal ISP de Venezuela y está gestionado por el Estado. (Da servicio al 55,92% de los usuarios de Internet, incluida la banda ancha móvil dedicada, según CONATEL). En la mayoría de los casos, sólo es posible acceder a las páginas bloqueadas y evitar la censura utilizando una VPN. Esto sugiere que el gobierno pretende restringir el libre acceso de los ciudadanos a la información.

Y las restricciones suelen ser exhaustivas o, al menos, intentan serlo. Por ejemplo, la página de inicio de la VPN TunnelBear no es la única página bloqueada (https://tunnelbear.com), ya que también se intentó alterar la funcionalidad de la aplicación bloqueando su API (https://api.tunnelbear.com/). En años anteriores,

este bloqueo de la API de TunnelBear afectó el uso normal de la VPN en Venezuela, ya que los usuarios no podían registrarse en la aplicación o iniciar una sesión, incluso si ya eran usuarios activos. Afortunadamente, el equipo de TunnelBear modificó el punto final de la API, permitiendo así a los usuarios venezolanos acceder de nuevo a una VPN funcional.

En el caso de Tor, aunque los usuarios pueden seguir utilizando Tor y Tor Browser, nuestras mediciones confirman que CANTV está bloqueando partes de la infraestructura de Tor en un intento insuficiente de hacerla inaccesible.

Los bloqueos se produjeron en medio de un aumento del bloqueo de sitios, incluidos medios de comunicación de alto perfil como el-nacional.com y lapatilla.com. CANTV bloqueó el uso de Tor directamente y utilizó muchos de los puntos de acceso alternativos disponibles, que se conocen como puentes. Específicamente, apuntó a los puentes que estaban preinstalados en Tor.

1er semestre 2023

El sitio web eldiario.com fue el primer dominio bloqueado del 2023, el bloqueo inició el 25 de enero en la estatal CANTV, el bloqueo es de tipo HTTPS Y DNS simultáneamente.
El 26 de abril inició el bloqueo al dominio de Salario Digno VZLA, un sitio perteneciente a la Red Sindical Venezolana que tiene la finalidad de exigir salarios y condiciones dignas de trabajo. Este bloqueo está implementado por los proveedores CANTV, Digitel e Inter de tipo DNS y Movistar lo hizo de tipo HTTPS/HTTP.

La página del Observatorio de Finanzas se encuentra bloqueada desde el 3 de mayo por CANTV, Movistar, Digitel e Inter, en Movistar la modalidad del bloqueo es HTTPS/HTTP +DNS, mientras que los otros 3 proveedores aplicaron solo bloqueo DNS.
Los dominios focoinformativo.com y www.opinionynoticias.com se encuentran bloqueados únicamente movistar, en el primer dominio el bloqueo es de tipo HTTPS/HTTP+DNS y de tipo HTTPS/HTTP en el segundo caso, esto bloqueos son implementados directamente para dominios que terminen en informativo.com y noticias.com respectivamente, por lo que la pagina noticias.com tambien tiene activo bloqueo HTTPS/HTTP+DNS por movistar y ademas bloqueo DNS por CANTV, Digitel Inter y NetUno.

SITIO	DOMINIO	CATEGORIA	CANTV AS8048	Movistar AS6306	Digitel AS27717 AS264731	Inter AS21826	NetUno AS11562	SuperCable AS22313
El Diario	eldiario.com	NEWS	HTTPS+DNS	No	No	No	No	No
Salario Digno VZLA	salariodignovzla.com	HUMR	DNS	HTTPS/HTTP	DNS	DNS	No	
Observatorio de Finanzas	observatoriodefinanzas.com	HUMR	DNS	HTTPS/HTTP+DNS	DNS	DNS	No	
Foco Informativo	focoinformativo.com	NEWS	No	HTTPS/HTTP+DNS	No	No	No	
Opinion y Noticias	www.opinionynoticias.com	NEWS	No	HTTPS/HTTP	No	No	No	
Noticias del Mundo	noticias.com	NEWS	DNS	HTTPS/HTTP+DNS	DNS	DNS	DNS	

Tabla que muestra los bloqueos de páginas iniciados en el primer trimestre de 2023, según lo registrado por VE sin Filtro. (Fuente: VE sin Filtro)

CONECTIVIDAD Y DISPONIBILIDAD DEL SERVICIO DE INTERNET

La conectividad a Internet en Venezuela puede describirse como intermitente. Los cortes y las interrupciones de la conectividad se producen con regularidad, dejando grandes franjas del país sin conexión. Por ello, la disponibilidad del servicio de Internet ha sido un problema para muchos usuarios. La dinámica económica y política del país ha afectado negativamente al desarrollo y mantenimiento de las infraestructuras de telecomunicaciones y del sistema eléctrico, de las que dependen casi todas las conexiones del país. Esto ha provocado que los servicios de Internet sean limitados y poco fiables a través de los años.

VE sin Filtro supervisa los niveles de conectividad en todo el país, informando de los cortes y otras interrupciones a gran escala de la conectividad a Internet. Los cortes, o más en general los incidentes de interrupción, pueden deberse a problemas técnicos de un ISP o a problemas de infraestructura más amplios, como un apagón, y son visibles mediante métricas de conectividad a nivel de ISP o estatal.

Los incidentes se clasifican en función de su nivel de gravedad (crítico, grave o leve) y de su origen, como un apagón o un fallo del ISP, o cortes intencionados de Internet si se producen. A veces, no se puede identificar el origen. Estas interrupciones del servicio de Internet son percibidas por los usuarios, que a menudo informan de interrupciones del servicio que duran horas y a veces días.

Cuando un incidente afecta a varios estados o ISPs, los consideramos "sucesos" independientes que forman un único incidente. Sin embargo, este análisis no incluye los fallos de servicio prolongados que duran semanas, meses o años.

Incidentes De Conectividad

En 2022, VE sin Filtro notificó un total de 86 interrupciones de la conectividad a internet, lo que evidencia un aumento del 83% de los incidentes registrados durante el 2021. En ambos años, el mes con mayor número de casos fue febrero, con un total de 16 incidentes en 2022. En febrero de 2022, 8 de los incidentes tuvieron su origen en el ISP NetUno, que informó de múltiples interrupciones entre el 12 y el 17 de febrero. Cuatro de los incidentes se debieron a cortes eléctricos y se desconoce la causa de los otros 4.
Agosto de 2022 fue el mes con el siguiente mayor número de incidentes, 12, de los cuales 5 fueron causados por apagones y 2 por interrupciones del servicio a nivel de ISP. Se desconoce la causa de los otros 4 incidentes.

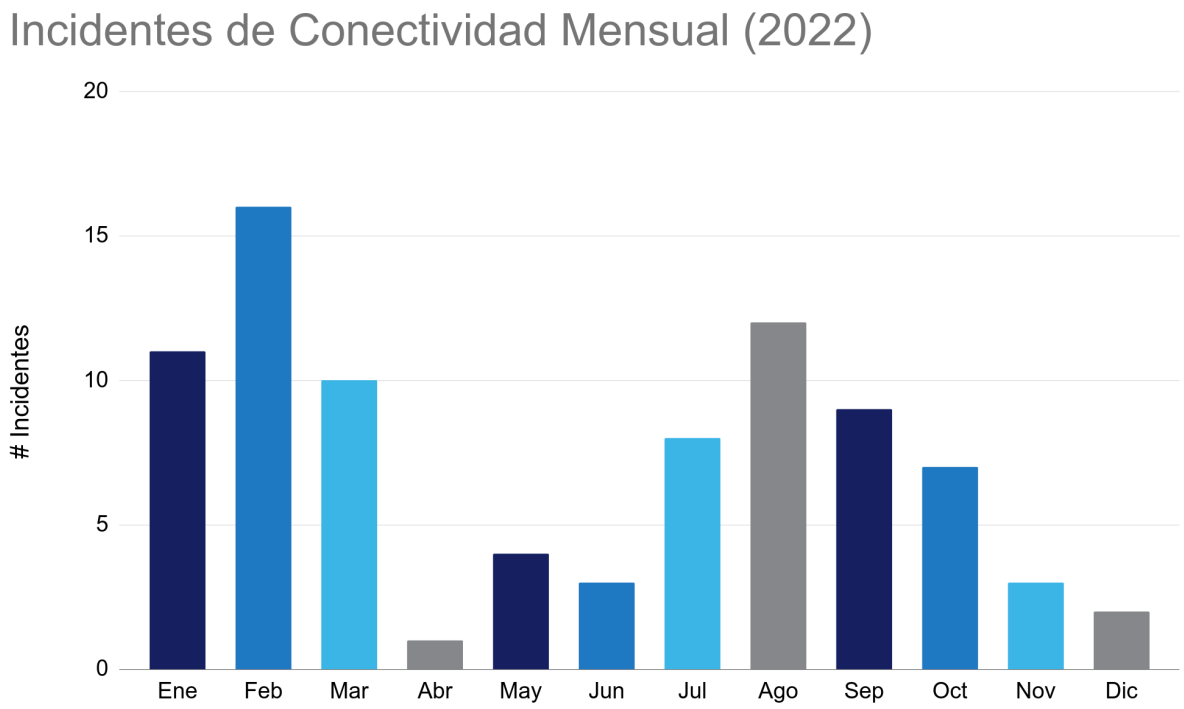


Gráfico de barras que muestra el número de incidentes de conectividad mensualmente de 2022. (Fuente: VE sin Filtro)

En 2022 hubo 474 eventos regionales. Táchira fue nuevamente el estado más impactado, con 43 eventos, seguido por 39 eventos en los estados Barinas y Trujillo y 37 en Mérida.

En el boletín de Agosto de 2022[3] del OSVP revela que las ciudades de San Cristóbal y Mérida presentaron el mayor porcentaje de usuarios con reporte de interrupciones diarias del servicio de Internet, con 61% y 52,8%, respectivamente.

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

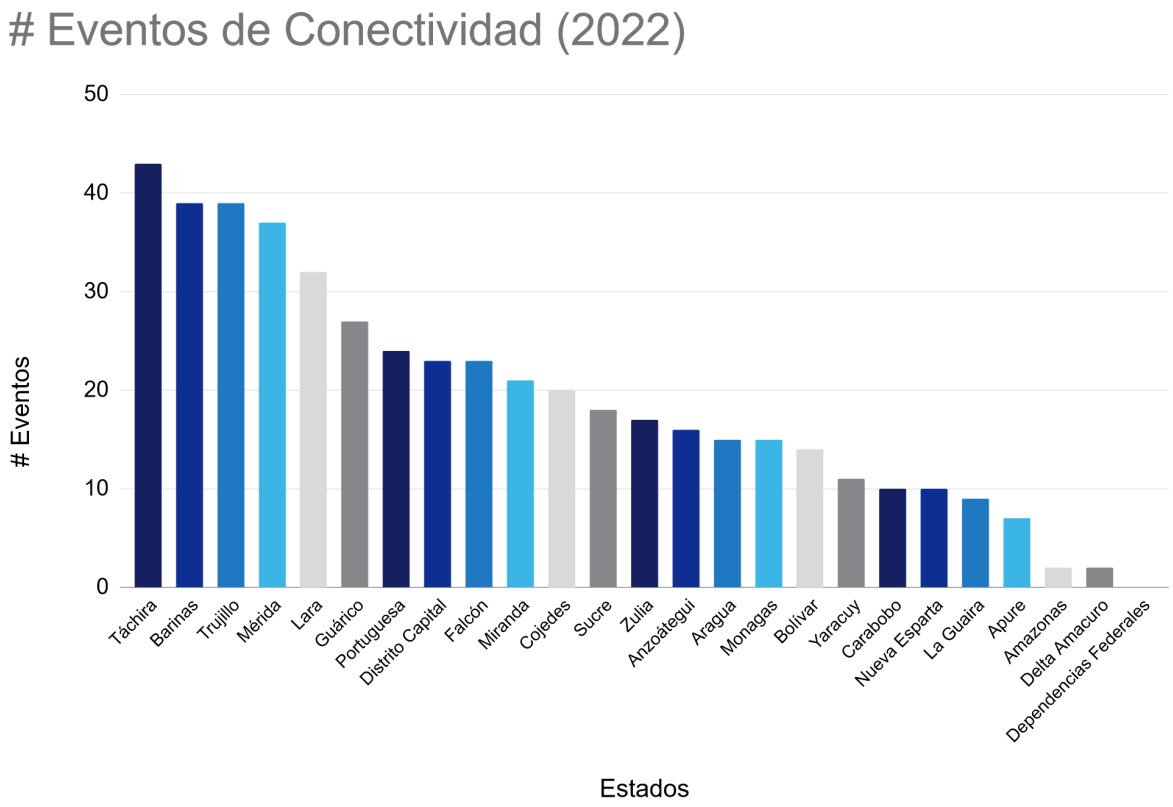


Gráfico de barras que muestra el número de incidentes de conectividad por estado de 2022. (Fuente: VE sin Filtro)

Eventos Según La Magnitud Del Incidente

Las caídas de los niveles de conectividad en comparación con lo habitual se describen según su magnitud. Este trabajo ha sido categorizado por VE sin Filtro:

- **Crítico:** 0-50%
- **Serio:** 51-80
- **Leve:** Caída que no es inferior al 80% pero que coincide con un evento claro de disminución de conectividad en varios estados.

En 2022, Táchira y Mérida tuvieron el mayor número de eventos críticos(21 y 19 respectivamente) y fueron seguidas por Monagas (12), Bolívar (11) y Barinas (9), En el 2021 Táchira y Mérida también tuvieron el mayor número de eventos críticos. Mientras que Barinas tuvo el mayor número de eventos graves con un total de 21, luego le sigue Trujillo con 16 eventos graves, y después están Guárico y Lara con 14 eventos graves ambos estados. Con respecto a los eventos leves en Distrito Capital se registraron 19 eventos, siguen Trujillo y Lara ambos con 17 eventos, Miranda tuvo un total de 15 eventos leves, finalmente Portuguesa y Mérida ambos tienen un total de 12 eventos cada uno. En el 2021

Dado que los estados Amazonas, Apure y Delta Amacuro, mayoritariamente rurales, y las Dependencias Federales (denominación oficial de las islas menores en alta mar administradas desde Caracas) tienen los índices de penetración más bajos, detectar y medir las caídas de la conectividad a Internet es más difícil que en otros estados.

La mayoría de los eventos fueron leves con un total de 191, luego siguen los graves con 167 eventos y los críticos tiene un total de 116 eventos a nivel nacional.

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

Tabla que muestra el número de incidencias de interrupción de la conectividad por estado y nivel de gravedad de 2022. (Fuente: VE sin Filtro)

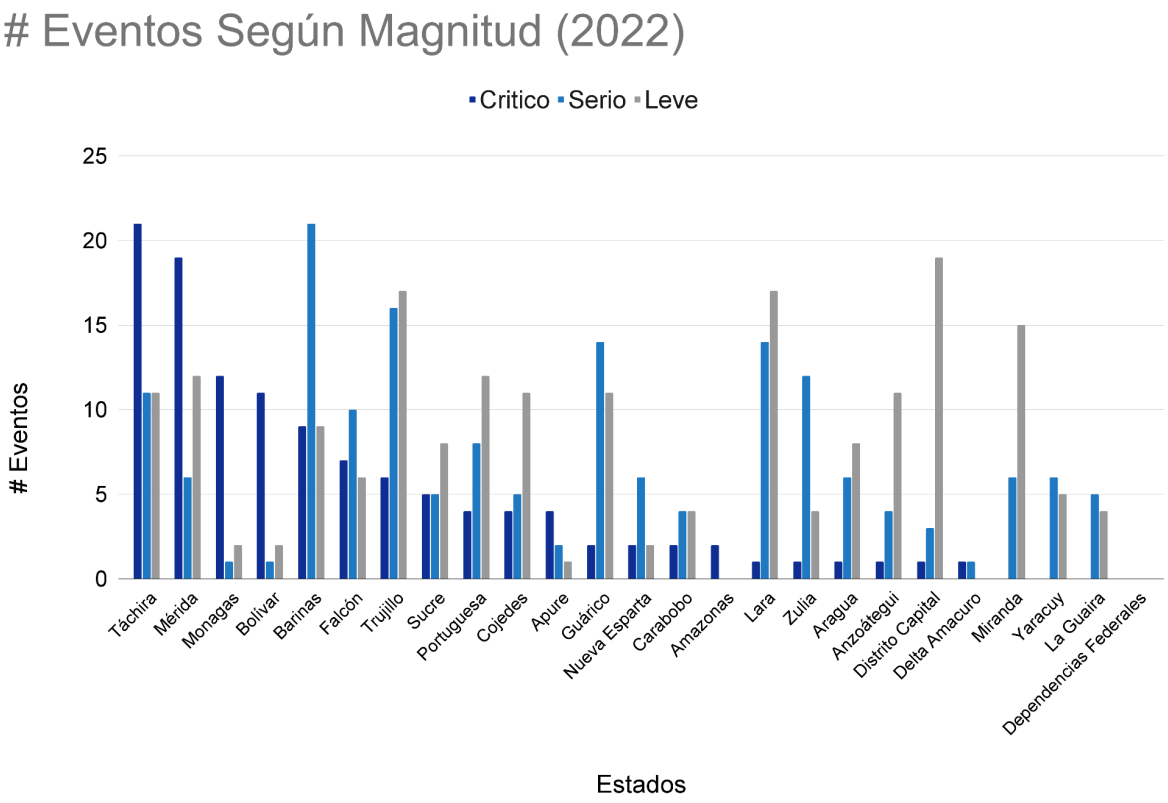


Gráfico de barras que muestra el número de eventos de conectividad por tipo (corte eléctrico, originado por el ISP u otro) de interrupción por estado o distrito venezolano de 2022. (Fuente: VE sin Filtro)

Según El Tipo De Falla

En cuanto al origen de los incidentes, VE Sin Filtro identificó apagones o caídas de tensión; fallos causados por los ISP, en su mayoría debidos a cables de fibra óptica de la red troncal dañados o problemas de servicio no definidos; y "otras causas", que son incidentes de origen desconocido.

En 2022 disminuyeron los incidentes de interrupción de la conectividad por cortes eléctricos en comparación con el año 2021. Con respecto al total de los eventos registrados, el 34,88% fueron a causa de cortes eléctricos, es decir 201 eventos. Los estados más afectados son Táchira, Trujillo, Barinas, Mérida, Portuguesa y Lara. Táchira, Mérida y Trujillo han aparecido en estas listas todos los años.

Las interrupciones de conectividad causadas por apagones eléctricos han sido una constante desde marzo de 2019, cuando un apagón nacional dejó a la mayor parte de Venezuela sin electricidad durante aproximadamente una semana, y en algunos lugares incluso más tiempo. Esta tendencia refleja la vulnerabilidad del sistema eléctrico de Venezuela, cómo el acceso a Internet generalmente depende de la red eléctrica y la necesidad de mantener y mejorar esta infraestructura. Desde entonces, Venezuela se ha enfrentado a una crisis energética que ha provocado apagones recurrentes en todo el país y ha producido muchos de los incidentes descritos.

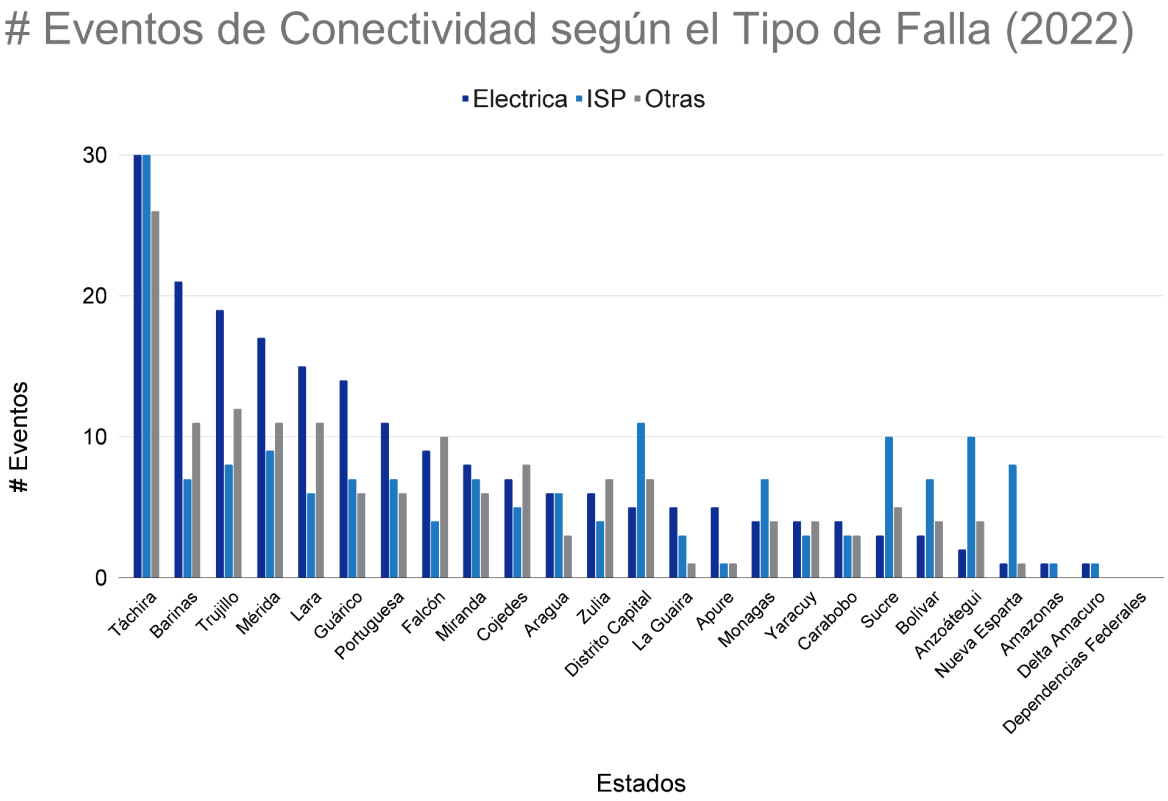


Gráfico de barras que muestra el número de eventos de conectividad por tipo (corte eléctrico, originado por el ISP u otro) de interrupción por estado o distrito venezolano 2022. (Fuente: VE sin Filtro)

El 14 de febrero de 2022 se produjo un apagón nacional que duró casi un día entero. Causó una interrupción de la conectividad en 23 estados durante 19 horas y 20 minutos. El incidente comenzó a las 12:50 a.m. El nivel de conectividad más bajo registrado a nivel nacional fue de 37% en comparación con los niveles normales, lo que se califica como una caída crítica de la conectividad. Otros 23 incidentes presentaron un nivel de conectividad de entre el 0 y el 50 por ciento de los niveles normales.

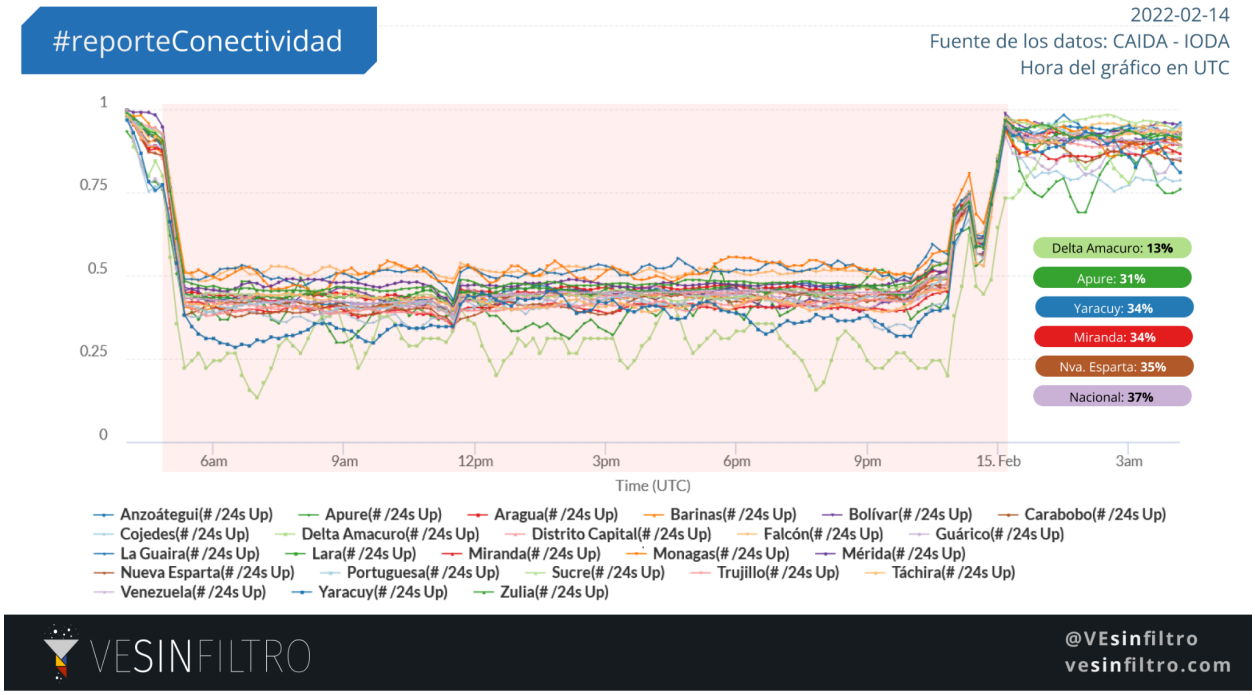


Gráfico lineal compartido en redes sociales que muestra la caída en la conectividad de la mayoría de los estados de Venezuela el 14 de febrero de 2022. Esta señal de conectividad es el número de segmentos IP /24 accesibles mediante sondeo activo, normalizado. (Fuente: VE sin Filtro, con datos obtenidos de la API de IODA)

En relación a los incidentes identificados por fallas del operador o proveedor de servicios, en 2022 hubo un aumento con respecto al total de incidentes por falla de ISPs de 2021, que fueron 8, mientras que para el 2022 el 34,88% de los incidentes fueron de este tipo, lo que significa que son 30 el total de estos. El estado Táchira volvió a ser el más afectado, con 30 eventos en este caso, es decir todos los incidentes de este tipo afectaron al estado Táchira.

Los incidentes debidos a otras causas, de origen desconocido representaron 30,23% del total de incidentes de 2022, ascendiendo a 26 incidentes. En 2021 sólo se registraron 11 incidentes de este tipo y Táchira tuvo el mayor número de eventos con un total de 26.

Según La Duración Del Incidente Y Los Eventos

Los incidentes a nivel nacional de 2022 duraron un total de diez días, doce horas y cincuenta minutos (para todas las interrupciones de conectividad regionales registradas). Los estados con mayor tiempo de fallas totales de conectividad fueron Táchira (ocho días, una hora y treinta minutos), Trujillo (siete días, veintiún horas y diez minutos) y Barinas (siete días, dieciséis horas y veinte minutos). Mientras que los demás estados se vieron afectados dentro de un rango de duración de entre 7 días y 3 horas.

Duration of Connectivity Events (2022)	
	2022

Estados	Duración (Dias)	Promedio (Días)	MAX (Días)
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

Tabla que muestra la duración de los eventos de conectividad por estado de 2022, incluyendo la DURACIÓN total, la duración MEDIA y la duración MÁS LARGA. (Fuente: VE sin Filtro)

Táchira, estado fronterizo, fue de nuevo el más afectado en 2022, como refleja la duración total de los eventos.

Duración De Los Incidentes Críticos Y Serios

Haciendo un análisis de la duración de los incidentes críticos y serios tenemos que Barinas (6 días 59 minutos 2 segundos) es el estado con una sumatoria de 30 eventos críticos y serios en total, Mérida con 25 eventos totales con una duración total de 5 días 22 horas 30 minutos luego en total de duración le sigue Táchira con 5 dias pero una sumatoria de 32 eventos críticos y serios son los estados con mayor

sumatoria total de tiempo. El resto de los estados se encuentran en un rango de duración de entre 5 días y 3 horas.

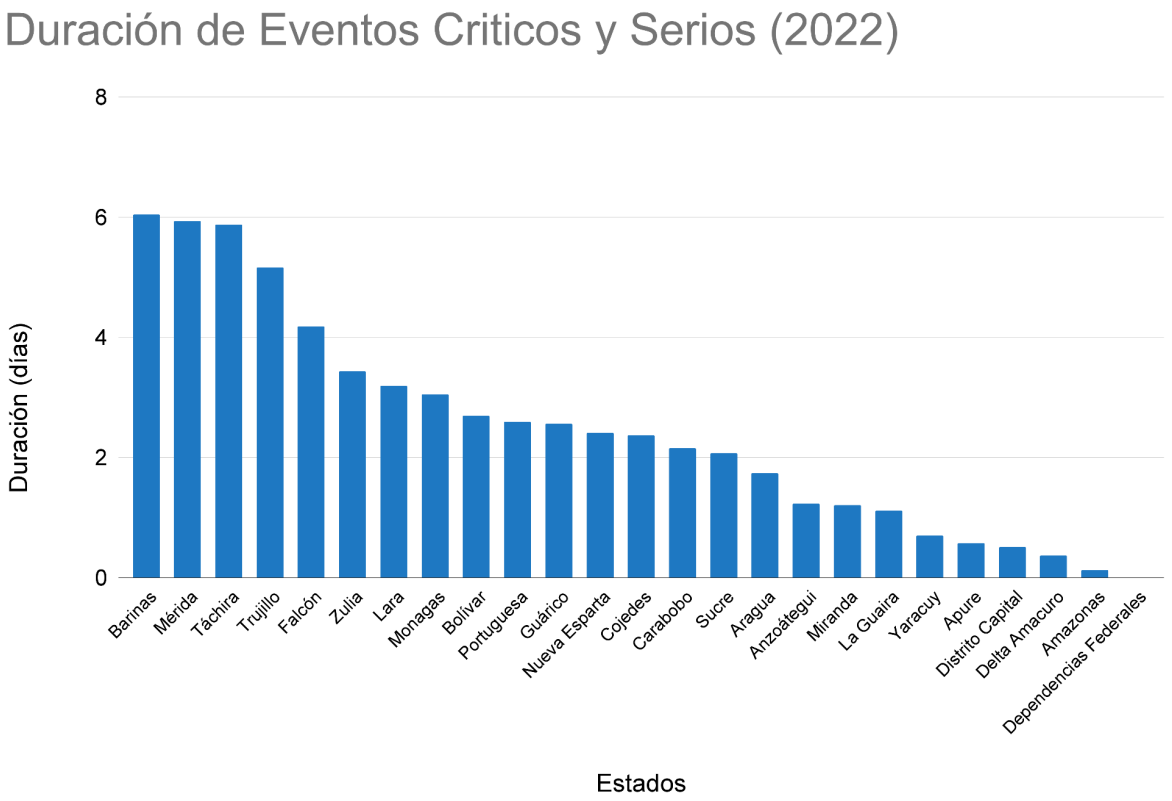


Gráfico de barras que muestra la duración (en días) de los eventos de conectividad por estado, de magnitud crítica y seria, 2022. (Fuente: VE sin Filtro)

Incidentes por falla de Isp y según la magnitud

La duración total de los eventos de falla de los ISP mostró que los ISP más impactados fueron la estatal CANTV y el proveedor privado NetUno. Las caídas de conectividad debidas a cortes de CANTV, confirmadas por el proveedor, representaron un total de siete eventos en 2021 y quince en 2022. Duraron un día y siete horas en 2021 y tres días y trece horas en 2022.

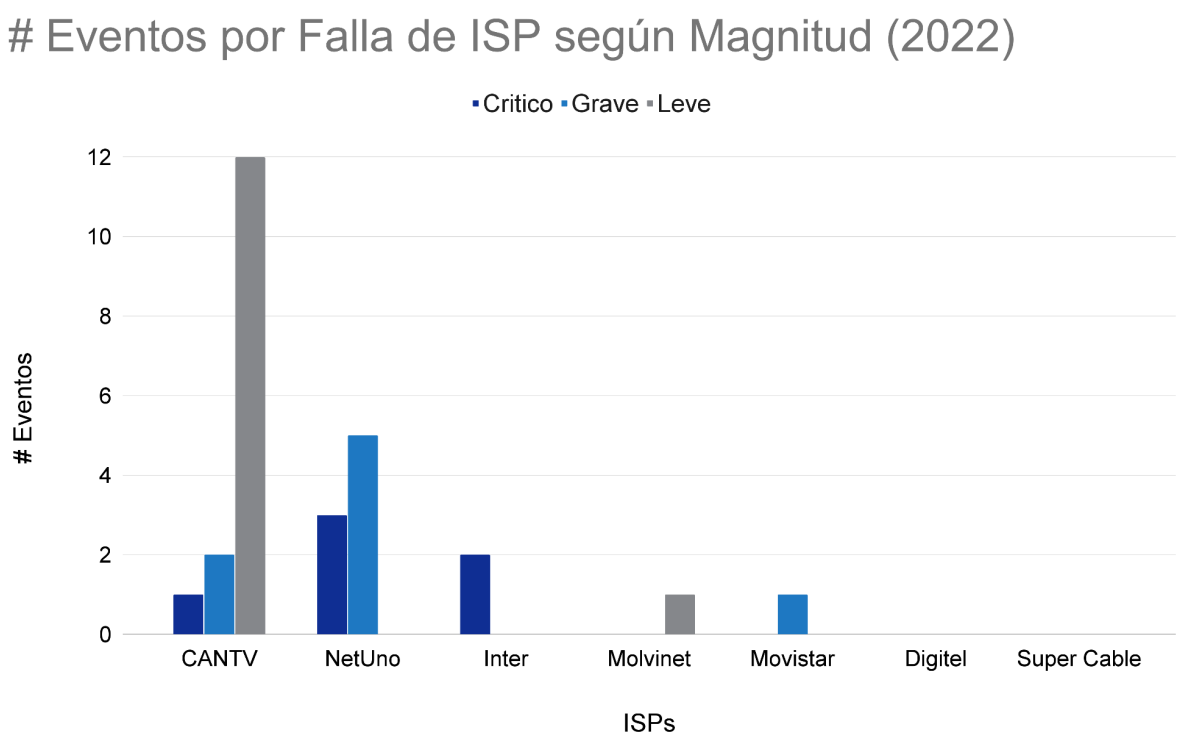


Gráfico de barras que muestra el número de eventos debidos a fallos del ISP por proveedor de 2022. (Fuente: VE sin Filtro)

El informe anual 2022 del Observatorio Social Humanitario sobre Monitoreo Comunitario de los Servicios Públicos señaló que el principal proveedor de Internet del país sólo puede garantizar que menos del 5% de quienes lo utilizan no experimenten cortes. Es importante considerar que CANTV en el último trimestre de 2022 tenía más de la mitad (55,92 por ciento) de los suscriptores del mercado de internet, según CONATEL. Con respecto a NetUno, hubo un aumento en el tiempo total de interrupción a dos días, veintitrés horas y diez minutos en 2022. Esto se debe a los 8 eventos de conectividad que tuvieron lugar en febrero de 2022, con una duración total de 5 días. Estos representan todos los eventos de caída de conectividad que afectaron a NetUno en 2022. Según el OVSP, NetUno presta servicios al 2,9% del mercado venezolano de Internet.

Gráfico lineal compartido en redes sociales que muestra la caída en la conectividad de NetUno durante el 12 al 18 de febrero de 2022. Esta señal de conectividad es el número de segmentos IP /24 accesibles mediante sondeo activo, normalizado. (Fuente: VE sin Filtro, con datos obtenidos de la API de IODA)

Duración De Falla Por Isp

Al sumar la duración de los incidentes por falla de ISP tenemos que la estatal nacional CANTV tiene un total de 3 días y 13 horas, le sigue NetUno con 2 días, 23 horas y 10 minutos, en tercer lugar está Inter con 4 horas y 30 minutos, le sigue Movilnet con 4 horas y 10 minutos y finalmente Movistar con 1 hora y 20 minutos de duración, mientras que Digitel y Súper Cable no presenta ningún evento a causa de falla propia.

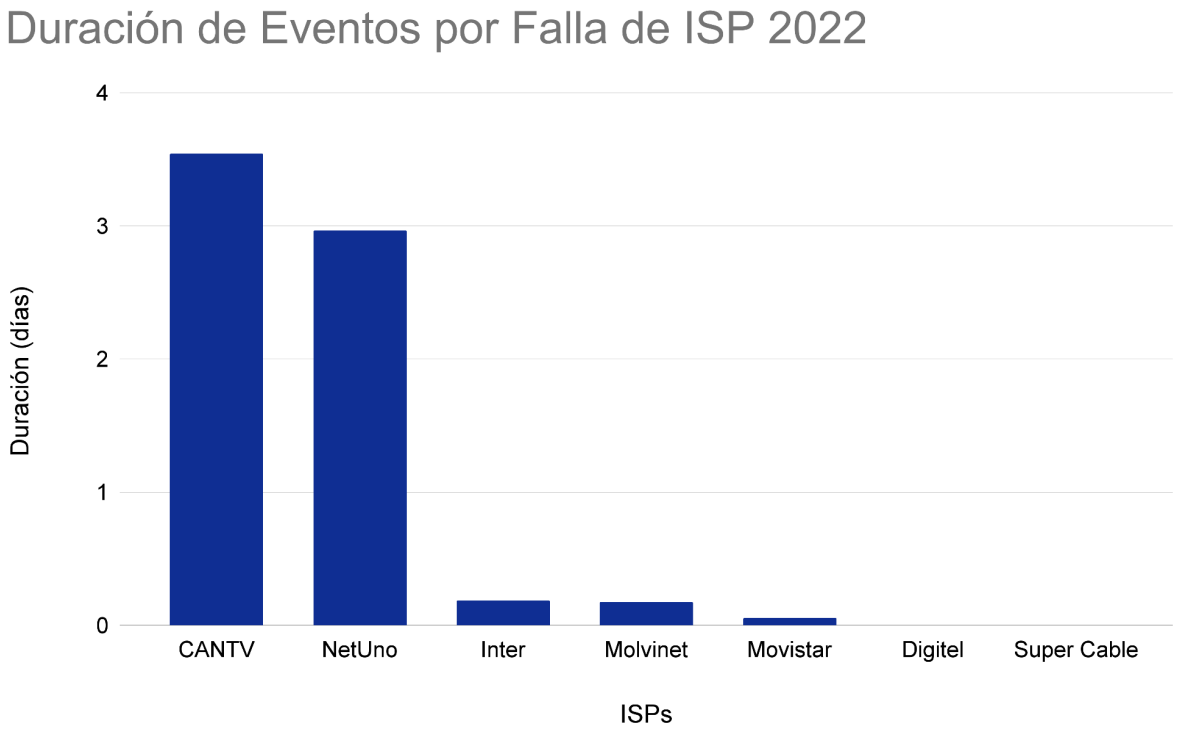
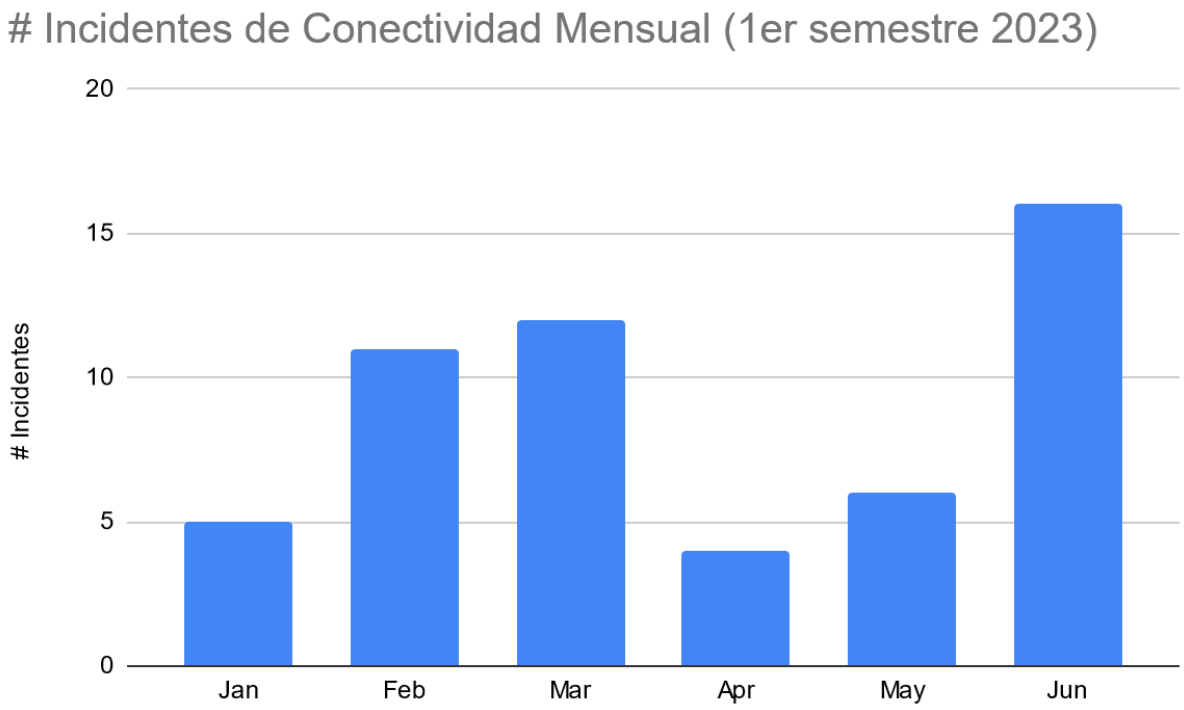
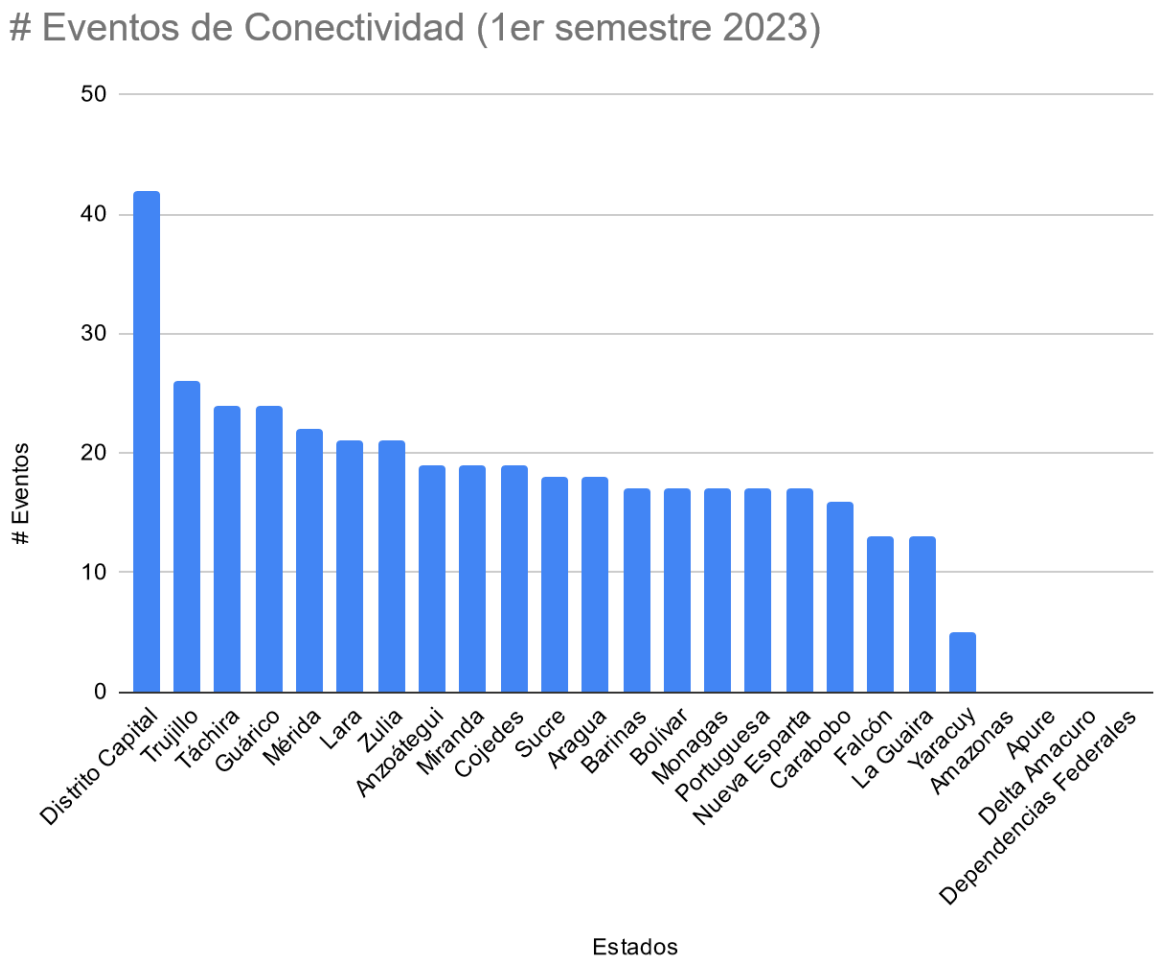


Gráfico de barras que muestra la duración, en días, de los eventos de fallo del ISP por proveedor de 2022. (Fuente: VE sin Filtro)

1er semestre 2023



Para el primer semestre del año 2023 VE Sin Filtro registró 54 incidentes de caídas de conectividad, en comparación con el total de incidentes del año 2022, en los primeros seis meses del año en curso se lleva 62,79% de los incidentes totales ocurridos durante 2022. El mes de junio de 2023 fue el que presentó mayor número de incidentes con un total de 16, luego le sigue marzo con 12 incidentes. Estos 54 incidentes son a su vez 405 eventos regionales 42 de estos eventos afectaron el Distrito Capital, luego entre los estados más afectados se encuentran los estados andinos Trujillo, Táchira y Mérida que tienen 26, 24 y 22 eventos de caída de conectividad regional respectivamente, el estado Guárico también es uno de los estados más afectados con 24 eventos al igual que el estado Táchira.



PROTECCIÓN DE DATOS PERSONALES Y SEGURIDAD DE SITIOS WEB DEL ESTADO

La protección de datos personales es fundamental para la seguridad de la privacidad de los usuarios y ciudadanos. A medida que más y más actividades se digitalizan, la protección de los datos personales se hace cada vez más importante.

La capacidad de las personas de poseer y controlar sus datos está consagrado en la legislación internacional de derechos humanos, incluida la Declaración Universal de Derechos Humanos y el Pacto Internacional de Derechos Civiles y Políticos. El derecho a la privacidad incluye la protección de los datos personales, y las personas tienen derecho a controlar cómo se recopilan, utilizan y comparten sus datos.

Los datos en sí deben tratarse como una propiedad y las personas deben recibir una compensación justa por ellos[4].

Todo lo que hace una persona deja rastros digitales que pueden revelar detalles íntimos de sus pensamientos, creencias, movimientos, asociaciones y actividades[5]. Los tribunales de derechos humanos también han reconocido que casi todos los pasos en el manejo de datos personales (desde la recopilación inicial hasta el uso, la conservación y el intercambio) pueden interferir con la vida privada. Esto significa que esas acciones deben limitarse a un objetivo legítimo[6].

Los gobiernos y las organizaciones deben garantizar y priorizar la protección de los datos personales de los individuos, estos se deben recopilar y procesar de forma transparente, consensuada y lícita, para que se respeten los derechos de las personas a la privacidad y a la protección de sus datos, evitando asi perjudicar a las personas o violar sus derechos. Esto significa que las personas deben ser informadas de qué datos se recogen, por qué se recogen y con quién se comparten. Las personas también deben tener la oportunidad de dar su consentimiento para la recogida y el tratamiento de sus datos.

Además de la transparencia y el consentimiento, las organizaciones también deben garantizar que los datos personales estén protegidos contra el acceso no autorizado, la alteración o la destrucción. Esto requiere la aplicación de medidas técnicas y organizativas adecuadas para garantizar la seguridad de los datos personales.

En Venezuela no existe legislación específica sobre privacidad o protección de datos, sin embargo, existen disposiciones aisladas en algunas leyes vigentes que regulan ciertos aspectos relacionados con la protección de datos, de forma insuficiente.

Al no existir herramientas para garantizar la protección de los datos personales; a falta de un marco jurídico y normas que los protejan, y frente a una actitud despreocupada de parte de los entes públicos y empresas privadas a hacer uso responsable de datos, proteger la información sensible, queda en manos de cada ciudadano. Es la forma de minimizar los riesgos del mal uso de sus datos o del acceso indebido por terceros.

Seguridad y confianza de sitios web del estado

Es responsabilidad de los entes públicos y privados que reciben información sensible de las personas, garantizar la seguridad de esa información de sus usuarios. Desde asegurarse de que sus servidores son seguros y los datos no son accesibles por terceros, hasta constatar que las cuentas de los usaurios pueden mantenerse seguras, igual que sus contraseñas, establecer protocolos de recuperación de contraseñas que no sean vulnerables al abuso y tomar medidas para asegurarse que los usuarios de sus sistemas puedan saber que están en un sitio genuino, especialmente en un contexto donde muchos

4

https://www.economist.com/open-future/2019/01/21/we-need-to-own-our-data-as-a-human-right-and-be-compensated-for-it

5 https://www.hrw.org/news/2018/04/19/data-privacy-human-right

6 https://www.weforum.org/agenda/2021/05/data-rights-privacy-human-rights/

usuarios acceden a sitios del Estado desde conexiones wifi públicas, conexiones administradas por terceros o equipos de otras personas

Una de las prácticas mínimas esperadas de los operadores de portales en Internet es que sus sitios web tengan un certificado TLS/SSL y operar bajo el protocolo HTTPS.

HTTPS proporciona cifrado para los datos transmitidos entre el navegador de un usuario y un sitio web, impidiendo que terceros intercepten y accedan a información sensible como contraseñas y datos de métodos de pago. Esta protección es especialmente importante para los sitios web que manejan datos sensibles, como los sitios de entidades públicas donde se manejan datos de identidad, hábitat, laboral, declaración de impuestos, entre otros datos proporcionados al realizar trámites públicos.

Los certificados SSL verifican la identidad del sitio web y garantizan que los datos transmitidos entre el usuario y el sitio web están cifrados y son seguros, lo que ayuda a mitigar los riesgos y amenazas asociados a los ciberataques y garantizar la tranquilidad de sus usuarios, como lo son: ataque man in the middle, ser objeto de phishing, manipulación de los datos transmitidos, entre otros.

La autenticación de dos factores es un método de seguridad que permite confirmar tu identidad al iniciar sesión, ya que la contraseñas son vulnerable a ciberataques, este método hace que acceder a tus cuentas sea más seguro. Ya que para poder iniciar sesión además de la clave debes ingresar una credencial, que puede ser algo que sabes, algo que tienes o algo que eres.

VE Sin Filtro analizó 279 dominios de sitios webs pertenecientes a entidades públicas, con extensión de dominio .ve, de los cuales al menos el 70% de los sitios no poseen certificado SSL, es decir la información transmitida y recibida por estas páginas no está encriptada. De esta lista de dominios 32 son sitios con manejo de información sensible, de los cuales 30 de tienen una sección de inicio de sesión, de estos hay 17 sitios en los que solo se puede tener una cuenta si eres autorizado previamente por el administrador del mismo, los 13 sitios restantes son páginas de login de uso público para realizar trámites fundamentales de los derechos de la ciudadanía, como la página del saime (siic.saime.gob.ve) que permite solicitar la cédula y el pasaporte, de los cuales casi la mitad (6 de estos) no posee certificados SSL lo q quieres decir que su información no se encuentra encriptada, con respecto a la autenticación de dos pasos solo uno posee la opción de activarla, que es el dominio para iniciar sesión en la petro app (petroapp.petro.gob.ve). Del total de los 32 dominios hay 2 de estos que son páginas de consulta de datos sensibles en las cuales no es necesario ingresar sus credenciales únicas y privadas, como la página del CNE (www.cne.gob.ve), donde puede consultar los datos de los votantes al ingresar la cédula de identidad, y la página del instituto venezolano de los seguros sociales (www.ivss.gov.ve), donde puedes consultar los datos de los ciudadanos con su numero de cedula y fecha de nacimiento, donde puedes obtener datos como nombre, lugar de trabajo, salario, fecha de ingreso al trabajo, y en el caso de las persona de la tercera edad puedes conocer el monto de la pensión que recibe y el banco donde se le deposita y si recibe más de una pensión.

Domain	Ente Publico	SSL	2FA
petroapp.petro.gob.ve	Petroapp	TRUE	TRUE
bdvenlinea.banvenez.com	BDVenlínea	TRUE	FALSE
persona.patria.org.ve/login/clave	Monedero Patria	TRUE	FALSE

siic.saime.gob.ve	SAIME - Trámites	TRUE	FALSE
tramites.saren.gob.ve	TRAMITES EN LINEA SAREN	TRUE	FALSE
vicesocial.info	Vicesocial Venezuela. Consulta por Cédula ACTUALIZADO 2023	TRUE	FALSE
emprenderjuntos.gob.ve/autenticacion	Emprender Juntos	TRUE	FALSE
www.cne.gob.ve	Consejo Nacional Electoral	FALSE	N/A
www.ivss.gov.ve	IVSS Instituto Venezolano de los Seguros Sociales	FALSE	N/A
certificacioninternacional.mijp.gob.ve	Certificación de Antecedentes Penales	FALSE	FALSE
contribuyente.seniat.gob.ve/iseniatlogin/contribuyente.do	SENIAT - Servicio Integrado de Administración Aduanera y Tributaria	FALSE	FALSE
legalizacionve.mppre.gob.ve	Sistema de Legalización y Apostilla Electrónica	FALSE	FALSE
put.intt.gob.ve/login.php	Planilla Única de Trámites - INTT	FALSE	FALSE
webpi.sapi.gob.ve/index0.php	WEBPI - Sistema En Línea de Propiedad Intelectual	FALSE	FALSE
www.imprentanacional.gob.ve/certificado_gaceta/site/	Sistema de Certificación de Gaceta	FALSE	FALSE
defensa-asegurado.sudeaseg.gob.ve	Sistema de Derechos y Defensa del Asegurado	TRUE	Login priv
fuerzalaboral.sudeaseg.gob.ve/ServidorFL/Proyectos/FuerzaLaboral/index.php	Fuerza Laboral	TRUE	Login priv
gsr.sudeaseg.gob.ve/login	SIS GSR	TRUE	Login priv
rtop.sudeaseg.gob.ve/DPCLC_2/Proyectos/DPCLC_2/index.php	sudeaseg	TRUE	Login priv
sefam.sudeaseg.gob.ve/Servidor/Proyectos/EstadosFinancieros/index.php	SEFA Sistema de Estados Financieros Analíticos SEFA	TRUE	Login priv
tvl.sudeaseg.gob.ve/login	SUDEASEG |UsuariosExternos	TRUE	Login priv
uam.edu.ve	Universidad Arturo Michelena	TRUE	Login priv
virtual.uvm.edu.ve	Universidad Valle del Momboy	TRUE	Login priv
www.inscripciones.uc.edu.ve	Universidad de Carabobo - DICES	TRUE	Login priv
aulavirtual.ujap.edu.ve	Plataforma Acrópolis / Universidad José Antonio Páez	FALSE	Login priv
dgpatrimonios.seniat.gob.ve/auth	SENIAT	FALSE	Login priv
elegibilidad.banavih.gob.ve	BANAVIH	FALSE	Login priv
faovel.banavih.gob.ve	FAOV	FALSE	Login priv
https://almccs.gob.ve/site/login.html	ALMACENADORA CARACAS	FALSE	Login priv
mcenlinea.snc.gob.ve	Sistema RNC	FALSE	Login priv
www.tsj.gob.ve	Tribunal Supremo de Justicia	FALSE	Login priv

Otro factor de seguridad analizado de estos sitios fue el proceso de recuperación o cambio de contraseña, por lo que se puede mencionar que el sitio de seniat en línea, tiene una opción antes de iniciar sesion que que es “Olvidó toda su información” en la cual te solicitan datos personales públicos del usuario como número de documento de identidad o RIF, además de otros datos que se encuentran en el RIF, el cual es un documento de consulta pública por lo que estos datos son de fácil acceso, lo que hace que terceros puedan cambiar o restablecer la cuenta de seniat en línea. El resto de los dominios que requieren inicio de sesión en su mayoría envían un código o clave temporal a tu correo electrónico para realizar el cambio de contraseña.

FALTA DE ACCESIBILIDAD COMO LIMITACIÓN AL EJERCICIO DE DERECHOS EN INTERNET

Limitaciones a personas con discapacidad

Es imposible negar la importancia del internet para la participación plena en la sociedad y el ejercicio de los derechos humanos, sin embargo las personas con discapacidad están seriamente desprotegidas, abundando portales web y fuentes de información, incluyendo algunas fundamentales del estado, no cumplen con estándares mínimos de usabilidad y accesibilidad.

Aunque para muchos la web y el internet en general se entiende principalmente como un medio visual, y que nuestra interacción con estos elementos visuales ocurre con nuestras manos y dedos, internet va mucho más allá. Aunque una persona vidente lea las palabras en una página web, una persona ciega podría, por ejemplo, usar software para leer el contenido de la página; una persona sorda podría ver un video en internet y leer sus subtítulos; o una persona con discapacidad motora podría pedirle a su equipo dónde hacer click en la pantalla verbalmente.

Cuando una página web o sistema está mal diseñado e implementado, crean dificultades que hacen los sistemas más difíciles de usar para todo tipo de usuarios, especialmente aquellos con discapacidad. Esto afecta a una población que no cuenta con garantías para ya es desproporcionadamente afectada por la crisis en Venezuela como ha sido documentado por organizaciones como CONSORVEN[7] identificado por el Comité sobre los Derechos de las Personas con Discapacidad y el Consejo de Derechos Humanos de las Naciones Unidas.[8]

La web y el internet en general es usada por incontables personas con discapacidad en todo el mundo, pero esto es posible gracias a sitios web, aplicaciones y sistemas bien diseñados, siguiendo prácticas de accesibilidad. Es responsabilidad del estado garantizar que el acceso a la información y servicios importantes en internet, especialmente la del estado, sean accesibles y usables.

La expansión en el acceso de teléfonos inteligentes ha ayudado a hacer algunas tecnologías asistivas más comunes en Venezuela, permitiendo el acceso a tecnologías y herramientas diseñadas para personas con discapacidad incluídas en el sistema operativo de estos dispositivos así como aplicaciones descargadas para este propósito. Sin embargo, el acceso a teléfonos inteligentes implica una barra de costo para algunas personas, algunas personas requieren adecuaciones distintas o adicionales y la efectividad de estas tecnologías depende en buena medida del buen diseño de sitios web, contenidos y aplicaciones tomando en cuenta mejores prácticas de accesibilidad para su uso con o sin el uso de estas tecnologías asistivas.

Por desgracia, servicios importantes en Venezuela tanto públicos como privados son muy difíciles o imposibles de usar de manera completa e independiente por personas con discapacidad, sin requerir asistencia de otras personas, mediante el uso de tecnologías asistivas.

Reportes de CONSORVEN muestran que el acceso a la información en internet se ve limitado por contenidos que no son accesibles, como videos informativos sin subtítulos o interpretación en lenguaje de señas. Otro ejemplo de contenidos poco accesibles son imágenes importantes para entender un documento o publicación sin descripción en texto o una infografía informativa sin un texto equivalente.

[7] Informe Anual 2022: Situación de los DDHH de las Personas con Discapacidad en Venezuela – CONSORVEN

[8] A/HRC/51/L.41
CRPD/C/VEN/CO/1

Por otro lado, la gran mayoría de las páginas del gobierno de Venezuela, y en especial la de portales necesarios para trámites gubernamentales esenciales como la solicitud de documentos de identidad, pago de impuestos, entre muchos otros, no siguen prácticas básicas de usabilidad y accesibilidad, dificultando a algunas personas su uso y posiblemente haciendo imposible su uso de forma privada e independiente a otras.

El sitio web del Servicio Administrativo de Identificación, Migración y Extranjería, por ejemplo, publica los instructivos de cómo utilizar la página para distintos trámites como videos con audio sin subtítulos ni interpretación en lenguaje de señas, la página no puede ser navegada por medio del teclado no hace posible la navegación por teclado para poder acceder a la página de inicio de sesión del sistema para gestionar sitas de trámites, entre otros problemas

Por su parte, la página del SENIAT, hace imposible su uso con un lector de pantalla ya que utiliza imágenes, en vez de texto, tanto para el encabezado de secciones como para hipervínculos y botones necesarios para operar la página. Las imágenes e hipervínculos no están etiquetadas, no tienen descripción ni título, haciendo imposible de operar con un lector de pantallas.

Incluso la página del El Consejo Nacional para las Personas con Discapacidad (Conapdis), que tiene funciones de accesibilidad que faltan en otros sitios del estado, carece de descripciones en texto de las imágenes que forman parte del contenido, para ser usadas por lectores de pantalla.

AMENAZAS A LA PRIVACIDAD

El derecho a la privacidad está seriamente limitado en Venezuela de múltiples formas, afectando a su vez el ejercicio de otros derechos, especialmente el derecho a la libertad de expresión. Las amenazas a la privacidad varían desde ataques informáticos sofisticados hasta la examinación de equipos como celulares y computadoras bajo coerción.

La privacidad de las comunicaciones, el rastreo de la actividad en redes sociales de los venezolanos y hasta la ubicación en tiempo real de las personas por medio del teléfono celular son una amenaza para cualquier ciudadano, pero especialmente afectan a periodistas, activistas, políticos y otros actores cívicos

La vigilancia y monitoreo de los ciudadanos a través de la tecnología a veces funciona como una gran red afectando de forma masiva a grandes cantidades de usuarios y otras veces altamente dirigida. Ocasionalmente utilizando múltiples métodos y tecnologías en una misma acción.

A pesar de las políticas de importantes plataformas internacionales de redes sociales de ignorar las solicitudes de información de usuarios por parte de las autoridades venezolanas, y una confianza generalizada en la capacidad de algunas empresas internacionales para mantener seguros los datos de los usuarios, un número creciente de startups locales utilizan y registran cantidades cada vez más grandes

de información personal que no tendrían la misma capacidad e interés de resistir solicitudes de datos del estado.

Monitoreo de redes sociales

De acuerdo con el Instituto Prensa y Sociedad de Venezuela, uno de los mecanismos de persecución contra periodistas que se ha instaurado en los últimos años es la persecución a través del uso del discurso estigmatizante, la criminalización de la labor periodística y campañas de desprestigio y desinformación a través de las redes sociales, entre otras plataformas.

A lo largo de 2022, esta organización totalizó 62 vulneraciones en la categoría de discurso estigmatizante, que representaron 28 incidentes de insultos o descalificaciones de funcionarios públicos o figuras influyentes, 18 actos de criminalización y 16 campañas sistemáticas de desprestigio y desinformación. Concretamente, estos hechos afectaron a 31 periodistas y 21 medios de comunicación. https://ipysvenezuela.org/2023/03/05/periodismo-bajo-las-sombras/

Por años, organizaciones de la sociedad civil han documentado represalias y persecución en contra de ciudadanos por el simple hecho de hacer uno legítimo de su libertad de expresión en internet, desde tweets públicos hasta por el contenido de sus estados en Whatsapp. La vigilancia de la actividad en línea de los venezolanos, especialmente en redes sociales y plataformas de mensajería como Whatsapp se apoya en parte también individuos alineados con el Gobierno y canales para reportar algunos de estos mensajes.

Aunque muchos mensajes críticos al Gobierno son transmitidos sin mayor consecuencia en redes sociales, el riesgo a la persecución por opiniones expresadas en internet tiene un efecto silenciador sobre ciertas críticas por personas, especialmente en espacios públicos para usuarios con cuentas identificadas abiertamente.

Un caso ilustrativo es el de Yohn Alejandro Noguera en junio de 2022, quién fue detenido[9] por la Guardia Nacional Bolivariana (GNB) después de que éste criticara a la GNB a través de WhatsApp. Posteriormente, Noguera fue acusado de "incitación al odio".

También en 2022, las autoridades venezolanas detuvieron[10] a Olga Mata, una usuaria de TikTok de 72 años, y la acusaron de delitos de odio tras publicar un vídeo satírico en el que se burlaba de Nicolás Maduro, su esposa Cilia Flores, Cabello y el fallecido Hugo Chávez.

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

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

El domingo 13 de noviembre de 2022, el Cuerpo de Investigaciones Científicas, Penales y Criminalísticas (CICPC) informó que detuvo[11] a dos personas por instigar al odio después de que hicieran comentarios despectivos sobre el presidente del Instituto Nacional de Hipódromos, y conocido miembro del partido gobernante, Antonio Álvarez. Los detenidos fueron identificados como Denys Jesús Custodio, de 34 años, y Robert José Yañez, de 57 años. Ambos utilizaron Twitter para hacer comentarios que supuestamente "denigraban" a Álvarez.

Ya es habitual[12] que funcionarios de Gobierno inicien casos motivados políticamente que resultan en la detención arbitraria de personas por expresar sus opiniones, como una forma de restringir la oposición política.

Espionaje e interceptación a las telecomunicaciones

El aparato estatal para la intercepción de las telecomunicaciones de los venezolanos es masivo, y quedó en evidencia a mediados de 2022 en un informe de transparencia de Telefónica, casa matriz de Movistar Venezuela, el más importante operador de telefonía celular en el país.

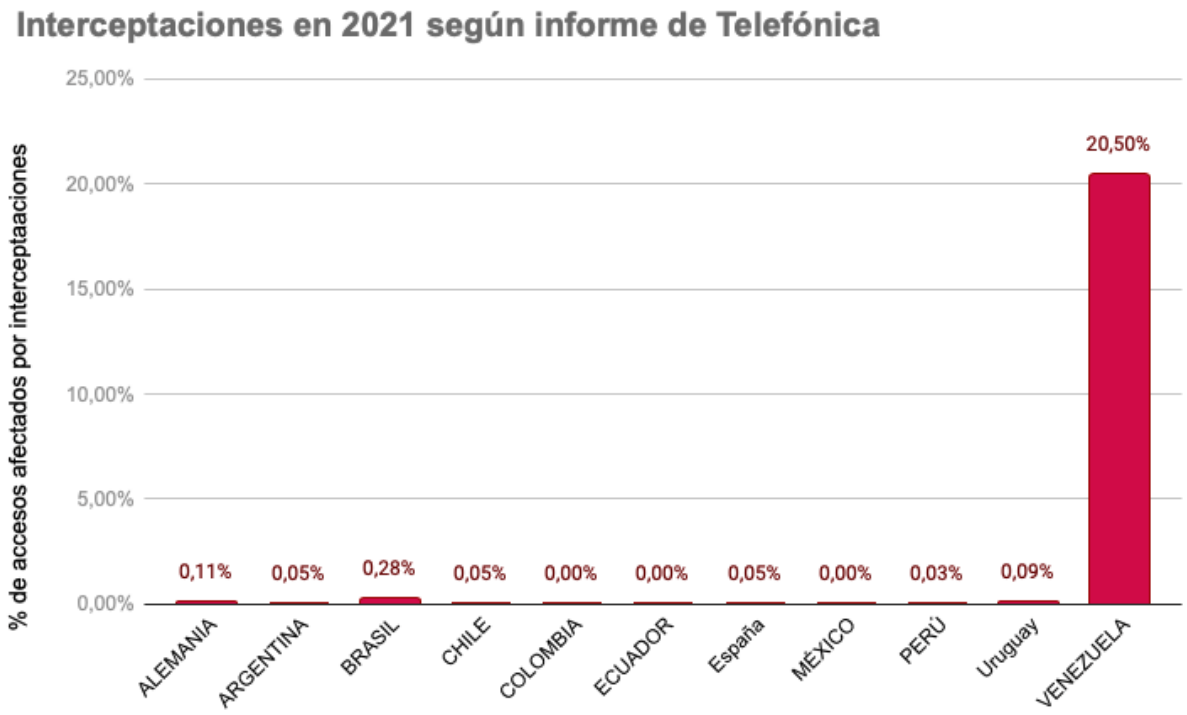
El informe indica que en 2021 Movistar interceptó las comunicaciones de 1 millón 584 mil 547 líneas de sus clientes en Venezuela, más del 20% de las líneas de teléfono o internet. Estas intervenciones se habrían hecho por órdenes del gobierno de Nicolás Maduro en una violación masiva del derecho a la privacidad. Movistar no ha vuelto a publicar un informe de transparencia similar hasta la fecha (Septiembre, 2023).

Las cifras de intercepciones por los otros operadores de telefonía y servicios de internet se desconocen, pues no presentan informes de transparencia, pero se debe asumir que son similares, o posiblemente peores en el caso de las empresas del Estado. La idea de que 20% o más de las líneas de telefonía o conexiones a Internet, en otras operadoras, también pudieran haber sido ser espiadas por el Gobierno de alguna manera es un prospecto altamente autoritario.

En contraste, las solicitudes de interceptación por otros países, en los otros mercados donde opera Movistar, no alcanzan 0.3% de las líneas en el peor de los casos.

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

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



Al mismo tiempo se pudo conocer:

- Líneas (accesos) afectados por la intercepciones: 1.584.547 (21% de las líneas)
- Líneas (accesos) afectados por solicitudes de metadatos: 997.679 (13% de las líneas)
- Accesos de líneas de teléfono y de servicio de internet de Movistar Venezuela: 7.730.000
- Tasa de líneas (accesos) afectados por solicitudes de ambos tipos: 33%
- El número de líneas (accesos) afectados por intercepciones aumentó 7 veces desde 2016, cuando eran 234.932 accesos afectados
- No reciben solicitudes de órdenes judiciales, sino de órganos de investigación, policiales, militares, inteligencia y hasta la universidad de seguridad UNES

Además de la entrega de metadatos de las telecomunicaciones, que en sí mismo es altamente sensible y privado, las interceptaciones pueden incluir la entrega del contenido de las llamadas telefónicas, el contenido de los mensajes de texto SMS, la ubicación de personas por sus teléfonos celulares o el monitoreo de su tráfico de Internet, sin dar cifras detalladas sobre cada uno.

Para Movistar Venezuela, las autoridades competentes para solicitar la interceptación de comunicaciones son: el Ministerio Público, el CICPC, cuerpos de policía “habilitados para ejercer atribuciones en materia de investigación penal” y extrañamente la Universidad Nacional Experimental de la Seguridad (UNES).

De manera similar, las autoridades competentes para exigir metadatos sobre las comunicaciones y datos de los suscriptores (cosas como: a quién llama un usuario, cuánto duran las llamadas, cuáles son los datos del suscriptor, etc) son muchas de las mismas, incluyendo organismos militares y policiales.

En ningún lado menciona que las órdenes vienen de tribunales o vienen con aprobación de jueces, como hacen en otros países, pareciendo dejar ver que estas son las entidades de las que han recibido estas solicitudes, nunca con la validación de tribunales.

En la legislación venezolana citada por Movistar, las solicitudes de interceptación deben ser aprobadas por un juez para que sean válidas, con excepciones particulares como el caso de urgencias y flagrancias, en las que el CICPC puede hacer el pedido, pero hasta en estos casos, debe ser notificado el Ministerio Público y constar en el expediente.

El abuso en la obtención de metadatos de comunicaciones es igualmente una violación de los derechos de las personas cuando no se hace de forma respetuosa a los DDHH. La ubicación de las personas, con quiénes se comunican, por cuáles vías, por cuánto tiempo y con qué frecuencia es información sensible igual que el contenido de dichas comunicaciones.

Los estándares internacionales de DDHH establecen que cualquier interceptación de comunicaciones (de cualquier tipo) debe cumplir al menos estas condiciones:

- Objetivo legítimo: Debe buscar un interés legal necesario en una sociedad democrática y respetuosa de los DDHH, como investigar un crimen
- Necesaria: No se debería utilizar una práctica que podría vulnerar derechos si no es necesaria para seguir esos fines legítimos
- Proporcional: Como el uso de vigilancia interfiere con los derechos humanos, se debe utilizar sólamente cuando esto es proporcional a la gravedad del crimen que se busca investigar, se debe tratar de minimizar la cantidad de datos obtenidos debe ser minimizada a sólo lo necesario, controlar el acceso a esta información sólo para los fines aprobados y desechar información que no es relevante
- Que esté adecuadamente sustentado por las leyes
- Bajo una orden judicial de un tribunal competente e independiente de la autoridad interesada en la vigilancia de las comunicaciones
- Permitiendo el debido proceso, notificando a la persona cuando sea posible y manteniendo transparencia del proceso
- La privacidad es un Derecho Humano fundamental e inalienable, que a su vez es clave para el libre ejercicio de la libertad de expresión y asociación entre otros derechos.

Videovigilancia

La videovigilancia en muchas ciudades de Venezuela representa una amenaza a la privacidad que no es suficientemente entendida y requiere más investigación. Hay poca o ninguna información disponible sobre las capacidades de los sistemas instalados y su capacidad para interactuar entre ellos.

El Estado venezolano ha invertido más de mil millones de dólares estadounidenses en proyectos de videovigilancia y respuesta a emergencias relacionadas.

Caracas y otras muchas ciudades venezolanas cuentan con cámaras de videovigilancia en red, ubicadas en lugares estratégicos. Algunas cifras oficiales mencionan un sistema de más de 30,000 cámaras, conocido como VEN-911, gestionado por el gobierno y establecido por un consorcio de empresas chinas

que incluye a Huawei, CEIEC y ZTE. Es probable que estos sistemas de videovigilancia monitoreen, rastreen y graben protestas u otras actividades políticas y posiblemente ayuden a localizar y seguir los movimientos de personas de interés para las fuerzas de seguridad.

Se desconocen las capacidades completas de los sistemas instalados en Venezuela. Hay cámaras que registran matrículas en las entradas y salidas de Caracas y posiblemente de otras ciudades, que las autoridades pueden utilizar para seguir el movimiento de vehículos; y algunos vehículos blindados, así como unidades móviles de comando de la Policía Nacional, incluyen sistemas de cámaras en un poste extensible.

El consorcio Huawei-CEIEC ha vendido sistemas en otros países bajo contratos que han incluido capacidades de reconocimiento facial, drones para vigilancia e integración de datos con geolocalización de objetivos. Un informe del New York Times reveló que los oficiales de inteligencia en Ecuador tienen acceso directo a las transmisiones de su sistema equivalente, ECU-911, a pesar de afirmaciones de que se utiliza exclusivamente para la seguridad pública.[13]

Sin embargo, este sistema del gobierno central es sólo una de las muchas fuentes de videovigilancia, ya que también se han establecido sistemas aparentemente gestionados por municipios. Más notablemente, en 2021, el alcalde del municipio de Chacao, en Caracas, anunció un nuevo sistema que incluía reconocimiento facial, sin más información relacionada con el uso de los videos, capacidades, políticas, procedimientos, quiénes tienen acceso a ellos y si se interconectan con VEN-911. La policía de Chacao detuvo en Junio de 2022 a un grupo de activistas políticos y los entregó al Grupo de Operaciones Especiales de la Policía Nacional,[14] lo cual sugiere una cooperación más estrecha con las fuerzas de seguridad nacionales en situaciones políticamente sensibles de lo que muchos suponían.

Existen otras cámaras de una clase similar entre espacios públicos y privados, como cerca de centros comerciales y plazas públicas, muchas de las cuales carecen de una propiedad clara, ya sea privada, municipal o de otro tipo.

Extracción de datos, borrado y revisión de equipos bajo coerción

En 2022 y 2023 sigue siendo común que las fuerzas de seguridad del Estado exijan acceso a materiales sensibles, datos y conversaciones en dispositivos digitales, como teléfonos celulares, computadoras y cámaras. Sin ningún procedimiento regular ni autoridad para esto.

Es común que dicho acceso ocurra en protestas o en situaciones donde la mala gestión del régimen de Maduro es evidente. Ejemplos de lugares o momentos en los que podría tener lugar tal acceso son: en largas filas para servicios, en instituciones de atención médica deterioradas o durante períodos de escasez de alimentos. Son oportunidades en las que las fuerzas de seguridad han obligado a periodistas, ciudadanos y activistas a permitir que revisen el contenido de sus dispositivos, o obligándolos a borrar

[13] https://www.nytimes.com/2019/04/24/technology/ecuador-surveillance-cameras-police-government.html
[14] https://elpitazo.net/politica/pintar-grafitis-la-razon-por-la-que-detuvieron-a-cuatro-jovenes-en-chacao/

material fotográfico o grabaciones, coartando seriamente la libertad de expresión e información; o simplemente practican una confiscación arbitraria, por no decir robo.

Hay un sub-reporte de este tipo de incidentes, pero organizaciones que defienden la libertad de prensa han documentado casos contra periodistas. Espacio Público documentó más de treinta y un casos en trece regiones de Venezuela entre enero de 2020 y agosto de 2021, dirigidos principalmente a periodistas, incluyendo dieciocho instancias de confiscaciones ilegales de dispositivos y trece intentos de revisar el contenido de los dispositivos bajo amenaza o mediante el uso de violencia. Además de estos riesgos, organizaciones como Venezuela Inteligente han encontrado evidencia directa de la extracción de datos de computadoras portátiles y teléfonos móviles de periodistas detenidos que tenían sus dispositivos bajo la custodia de fiscales e investigadores criminales.

Las personas en riesgo deben asumir que, en caso de detención, cualquier dispositivo que tengan en su posesión, y posiblemente dispositivos en su hogar u oficina, serán examinados y se extraerán datos de ellos en el momento de una detención legal o ilegal. También deben esperar que las fuerzas de seguridad obtendrán, mediante medios coercitivos, cualquier contraseña que proteja esos dispositivos o servicios en línea.

Adicionalmente, las autoridades venezolanas han adquirido unidades Cellebrite UFED Touch a lo largo de los años, a pesar de las sanciones. Estos dispositivos se utilizan para hackear teléfonos móviles bloqueados y extraer datos de ellos. Se sabe que las autoridades venezolanas, incluida la Dirección General de Contrainteligencia Militar (DGCIM), los utilizan.

La extracción subrepticia de datos de sus dispositivos digitales puede ocurrir siempre que una persona pierda el control físico, incluso temporalmente, a la custodia de las fuerzas de seguridad. Esto incluye cuando se ingresan a instalaciones seguras donde los dispositivos no están permitidos, pero también durante breves interrogatorios y otros escenarios similares.

Más recientemente hemos observado casos de inspección de equipos junto a las víctimas y que oficiales lleven estos equipos desbloqueados a otro cuarto, posiblemente para realizar extracción de datos, durante interrogatorios irregulares a múltiples miembros de distintas organizaciones de la sociedad civil al cruzar la frontera aérea en aeropuertos internacionales.

ATAQUES DIGITALES

Phishing y robo de cuentas.

En el pasado se han identificado cómo el Estado venezolano ha usado el phishing en contra de periodistas, disidentes y activistas, usando desde ataques altamente dirigidos hasta varias campañas masivas altamente sofisticadas que manipularon el tráfico de Internet de todo un proveedor y se estima que afectaron decenas de miles de víctimas.

En 2019 y 2020, VE sin Filtro expuso dos grandes campañas de phishing organizadas por el Estado, una dirigida directamente contra disidentes y activistas venezolanos[15] y la otra contra usuarios de una plataforma de ayudas sobre COVID liderada por la oposición a Nicolás Maduro..

Estos ataques emplearon equipos sofisticados para inspeccionar todo el tráfico de los usuarios de CANTV, que comprende más del 70% de las conexiones a Internet residenciales, y manipular el tráfico de Internet para dirigirlos a una réplica falsa del sitio web que intentaban visitar, incluso si escriben correctamente el nombre de dominio de la página genuina.

VE sin Filtro publicó en el reporte de uno de esos casos una lista de sitios web maliciosos que incluían el dominio de nivel superior de Venezuela (.ve). Todos estos sitios estaban alojados en el mismo servidor utilizado en otra campaña de phishing atribuida a actores estatales venezolanos.

Aunque no se han documentado nuevas campañas de phishing a gran escala como estas, es una amenaza constante. El control sobre CANTV, la empresa de telecomunicaciones del Estado, y el poder de coacción sobre las empresas privadas, se presta para ataques de phishing y el acceso no autorizado a cuentas de servicios en línea. Una de las formas más comunes es, interceptando el SMS de verificación de dos pasos o recibiendolo luego de adquirir un nuevo SIM para la línea de la víctima.

Sin embargo el phishing de parte del Estado no es el único riesgo, una tendencia que comenzó en 2019 pero ha seguido en 2022 y 2023 es el robo de cuentas, especialmente de Whatsapp, la principal herramienta de comunicación usada en Venezuela. Periodistas y defensores de derechos humanos y ciudadanos en general, se han visto afectados por el robo de cuentas de WhatsApp.

Este robo de cuentas principalmente ocurre con fines criminales, pero pone en riesgo datos sensibles a terceros al tener acceso al whatsapp de las víctimas, permitiéndoles además suplantar su identidad. En un ambiente políticamente polarizado. Es posible que de esos ataques de phishing los criminales lleven información sensible, que parezca valiosa, a las autoridades.

De especial preocupación es la posibilidad de que fuerzas de seguridad e inteligencias estén siguiendo estas mismas técnicas para acceder a las cuentas de Whatsapp de personas perseguidas, defensores de derechos humanos, periodistas y activistas; pero sea difícil distinguir el origen y motivación del ataque; o que ocurra sin interacción alguna de la víctima mediante la intercepción de mensajes o el cambio de SIM.

Ataques y hackeo a servidores

Los ataques a la infraestructura digital, como los servidores web, son otra amenaza común contra organizaciones en Venezuela. El tipo de ataque más habitual es el ataque de Denegación de Servicio (DoS, por sus siglas en inglés) contra sitios web de organizaciones mediáticas.

En un ataque DoS, un actor malicioso genera un volumen extremo de tráfico hacia el servidor web objetivo hasta que este no puede responder a las solicitudes legítimas de sus usuarios, debido al abrumador volumen de peticiones de tráfico. Este tipo de ataque puede llevarse a cabo de diversas maneras,

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

incluyendo dispositivos propiedad del atacante, utilizando dispositivos de terceros comprometidos o incluso contratando el servicio de grupos delictivos. Un ataque DoS también puede convertirse en un ataque de Denegación de Servicio Distribuido (DDoS) si el tráfico proviene de un gran número de dispositivos coordinados en lugar de unas pocas fuentes más grandes.

Se han reportado ataques DoS por parte de muchos medios de comunicación y suelen coincidir con una noticia de última hora que le interesa silenciar al Gobierno o a intereses empresariales relacionados. Si los actores detrás de un ataque logran incapacitar o deshabilitar completamente un servidor web mientras una noticia nueva o viral está en el centro de atención, el impacto del informe se reducirá.

Algunos ataques DoS parecen motivados por intereses económicos y empresariales, mientras que otros se realizan por razones políticas, como cuando una noticia expone prácticas empresariales corruptas o es políticamente hostil al perpetrador.

En varios incidentes de supuestos ataques DoS, VE sin Filtro determinó, en consultas privadas, que las organizaciones afectadas a menudo tenían otros problemas subyacentes con sus servidores o sitios web, que se agravaba con el tráfico superior al normal o con un verdadero ataque DoS que de otra manera sería más fácil de manejar. Sin embargo, esto no resta importancia a los numerosos y graves ataques DoS contra medios independientes en Venezuela, sino que más bien ilustra las complejas vulnerabilidades y los recursos limitados de las organizaciones que trabajan en este contexto.

Las organizaciones en riesgo deben asegurarse de que sus sitios web y otros sistemas sean seguros. Algunos sitios web venezolanos han afirmado haber sido víctimas de hackeos dirigidos, en los que los atacantes obtuvieron acceso administrativo a los servidores web de su organización, extrajeron datos, eliminaron información o solicitaron algún tipo de rescate. Este es un riesgo grave; sin embargo, algunos de los incidentes observados, en lugar de ser hackeos dirigidos, fueron ataques DoS, ransomware o ataques que encuentran y comprometen sistemas vulnerables automáticamente. Los servidores desactualizados o mal configurados han sido un problema, como se ha observado en múltiples ocasiones por VE sin Filtro.

Remoción de contenidos de internet

Las políticas de las plataformas en Internet y la capacidad de respuesta a las solicitudes de terceros, repercuten en el trabajo para la comunicación en línea y para las actividades de las organizaciones de la sociedad civil, los periodistas y los medios de comunicación.

Cada vez más, las organizaciones de la sociedad civil y los medios de comunicación independientes de Venezuela se han enfrentado tanto a falsas amenazas legales como a contenidos inocuos que se divulgan de forma malintencionada.

En febrero de 2023, El Pitazo denunció que la empresa Eliminalia, encargada de gestionar la reputación de políticos, empresarios e incluso integrantes de grupos criminales, utiliza la reclamación de falsos derechos de autor para forzar la eliminación de contenido en línea para clientes privados, y es la misma empresa que ha hecho solicitudes a medios digitales venezolanos para que eliminen información relacionada con ciudadanos mencionados en notas o investigaciones por casos de corrupción.

Dice la nota que para conseguir su propósito, la firma recurre a distintas tácticas de desinformación. Una es el envío de peticiones a buscadores y compañías de alojamiento web que denuncian la falsa vulneración de derechos de autor, según detalla una investigación de la organización Forbidden Stories en su seriado ¨Story Killers¨.

De acuerdo con la ONG Freedom House, entre mayo de 2019 y marzo de 2021, Eliminalia realizó al menos 16 solicitudes fraudulentas a Google en nombre de clientes venezolanos para borrar contenidos por violar derechos de autor de acuerdo con la ley DMCA (Digital Milennium Copyright Act), una legislación aprobada en Estados Unidos en 1998.

Casos como el del sitio web de noticias La Gran Aldea (2020) y el de la organización no gubernamental Acceso a la Justicia (2021), que fueron retirados temporalmente, dejan en evidencia cómo solicitudes de retirada de DMCA afectan el ejercicio de derechos.

Las respuestas de las plataformas, especialmente las de Twitter y YouTube, a las sanciones y a la desinformación procedente de cuentas asociadas al régimen de Maduro han supuesto la desaparición de vídeos y otras publicaciones relevantes para las investigaciones sobre derechos humanos o a las que se hace referencia en informes internacionales sobre derechos humanos.

Algunos proveedores de software y servicios, como Adobe, se excedieron inicialmente en el cumplimiento de las sanciones a Venezuela, restringiendo temporalmente el acceso de los usuarios venezolanos; otros siguen bloqueando el acceso, lo que ha dado lugar a campañas de la opinión pública y de organizaciones de la sociedad civil. Muchas empresas internacionales de tecnología financiera dejaron de prestar servicios a clientes venezolanos, colocándolos en una situación aún más vulnerable.

Múltiples usuarios y organizaciones de medios independientes han visto sus cuentas de redes sociales sancionadas por violar las normas de la plataforma sobre noticias falsas e imágenes violentas, al cubrir, documentar o comentar las declaraciones de funcionarios públicos u otros eventos. A nivel proactivo, las plataformas deberían publicar guías más claras diseñadas para las organizaciones de noticias independientes sobre cómo pueden documentar contenidos nocivos sin infringir las normas y qué hacer si el contenido se retira injustamente.

Las plataformas deben asegurarse de que no están retirando contenidos o sancionando cuentas por cubrir y documentar responsablemente hechos noticiosos. En los casos en que se sancionen o limiten las cuentas de los medios de comunicación, o se retiren sus contenidos, lo ideal sería que las plataformas se pusieran en contacto con los medios para ayudarles a evitar suspensiones o la retirada de contenidos que documenten las acciones de funcionarios públicos.

En un ejemplo de este tipo, el canal de YouTube de El Pitazo fue prohibido en 2021 tras una serie de denuncias probablemente malintencionadas a vídeos en su mayoría antiguos, aunque el motivo exacto de la prohibición sigue siendo opaco. Más tarde, YouTube restableció la cuenta.

Intimidaciones, amenazas

El uso de redes sociales y otras plataformas en línea para acosar a mujeres y a otras comunidades

marginadas que comparten opiniones, al igual que a periodistas, está siendo cada vez más común. El Instituto Prensa y Sociedad de Venezuela (Ipys Venezuela) denomina este fenómeno como "acoso digital", especialmente cuando hay campañas para desacreditar y amenazar a periodistas. Aunque no hay registros cuantitativos de las violaciones que han ocurrido hasta la fecha, los investigadores han documentado ejemplos que muestran un aumento en las agresiones en este ecosistema desde 2019.

Los casos de violencia digital de género y su impacto en los derechos de las mujeres son significativos. Estas agresiones suelen incluir ataques con un alto contenido sexista y declaraciones que menosprecian las opiniones de una persona en función de su género.

Espacio Público abordó esta situación mediante la revisión de tres estudios de caso en mayo de 2022. Estos casos se centraron en las experiencias de Diana Liz Duque, una bióloga que investiga la conservación de especies silvestres, y las periodistas Gregoria Díaz y Lorena Arraiz.

Según Ipys Venezuela, funcionarios del Gobierno venezolano han replicado y ampliado la violencia que se origina en el espacio digital. La organización publicó un informe sobre el abuso al que fueron sometidas las periodistas mujeres ese mismo año, observando que sus derechos "principalmente son violados en las redes sociales". Cinco periodistas fueron víctimas de amenazas, declaraciones ofensivas y limitaciones en su privacidad.

Fuente	**Categoría**	**Numero de incidentes documentados**
		2022
IPYS Venezuela	Discurso estigmatizante	62
	Ataques y agresiones	55
Espacio Público	Intimidación	83
	Acoso verbal	44
	Amenazas	23

Tabla mostrando el número de incidentes registrados por categoría en 2022. Odio, discriminación y otras formas de abuso que pueden ocurrir en línea, según los datos registrados por Ipys Venezuela y Espacio Público. Los incidentes incluyen tanto los que ocurrieron en línea como fuera de línea (Fuente de datos: Ipys Venezuela y Espacio Público)