SIN DERECHOS EN #INTERNETVE

Reporte sobre la situación de los derechos humanos digitales en Venezuela

REPORTE 2022+2023

VESINFILTRO.ORG/2022+2023

ACCESO A INTERNET
CENSURA Y BLOQUEOS
VIGILANCIA Y PRIVACIDAD
ACCESIBILIDAD
ATAQUES DIGITALES
DATOS PERSONALES

VE SIN FILTRO

VE SIN FILTRO

CONEXIÓN SEGURA Y LIBRE

Sobre VE sin Filtro

VE sin Filtro es un programa dedicado al monitoreo y documentación de amenazas al ejercicio de los derechos humanos en el entorno digital en Venezuela de la asociación Conexion Segura y Libre.

Desde 2014 ayuda a identificar y evadir la censura en medios de comunicación y ha sido pionero en el uso conjunto de mediciones de red producidas automáticamente, mediciones por contribución de voluntarios y análisis de tráfico de red para documentar la censura en internet con criterio técnico. Así como el uso de investigaciones de fuentes abiertas para examinar restricciones a los derechos humanos en internet y atribuir ataques digitales a entidades públicas de Venezuela.

VE sin Filtro, junto al programa Conexión Segura, ofrecen ayuda de emergencia a organizaciones de la sociedad civil, periodistas y medios independientes bajo ataque o recientemente bloqueados; ayudando a solventar el incidente y mitigando el impacto de la censura.

Con evidencias técnicas y el análisis de datos, desvela y documenta el alcance de los bloqueos y la censura en internet, la vigilancia gubernamental indiscriminada y ciberataques contra la sociedad civil.

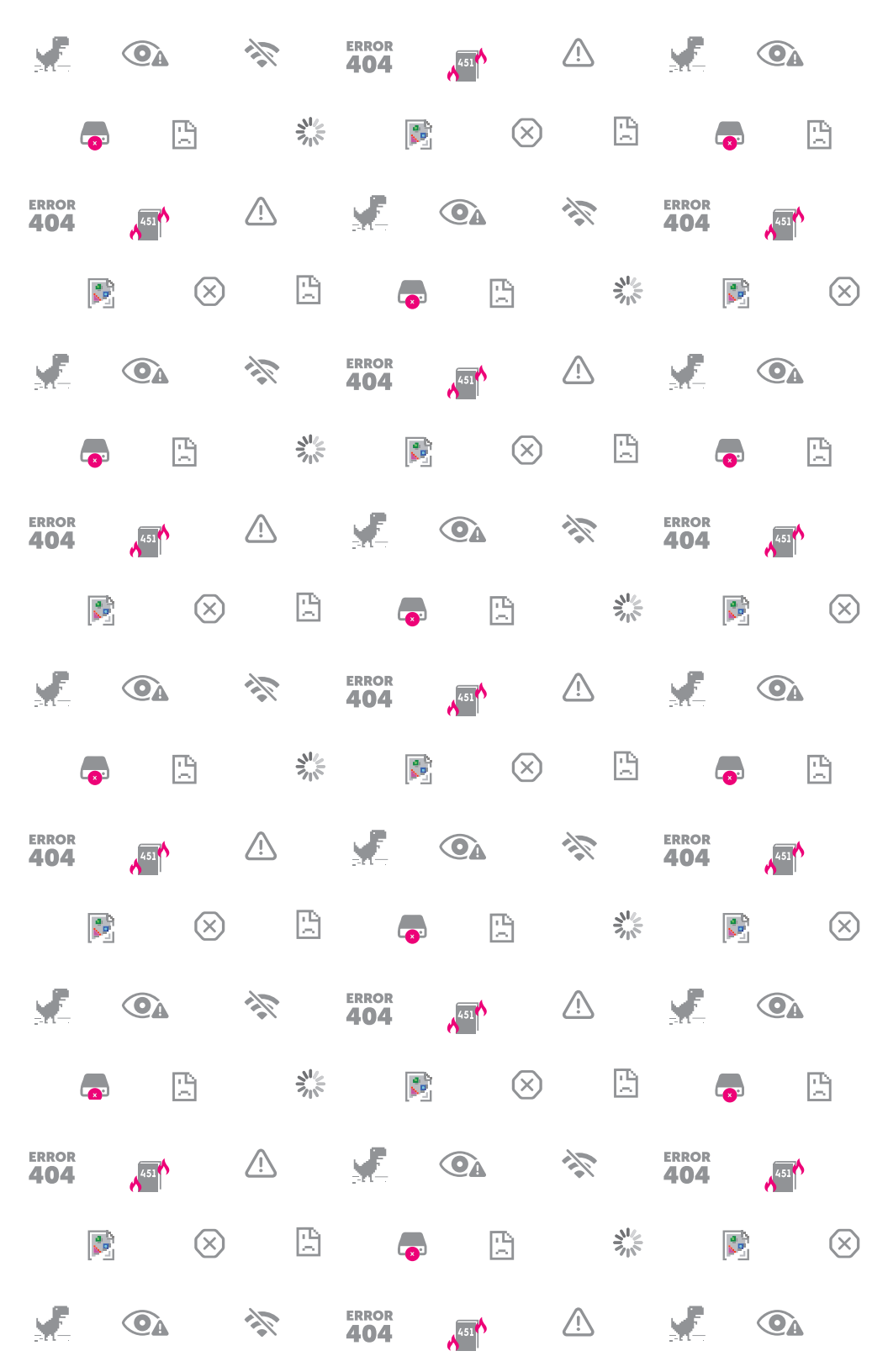
Mediante un monitoreo constante, VE sin Filtro provee actualizaciones en tiempo real sobre el estado del internet en Venezuela. Este trabajo no solo se enfoca en la conectividad y el acceso desiguala internet, sino también en el seguimiento a las interrupciones de servicio, "Internet Shutdowns", ataques y bloqueos, con el propósito de proteger el acceso a la información, la libertad de expresión, la privacidad, la seguridad, la educación, la participación, entre otros derechos fundamentales.

VE sin Filtro ofrece soporte y capacita a activistas, periodistas y organizaciones; elabora recomendaciones y prepara sobre mejores prácticas para contrarrestar las amenazas contra sus derechos y su seguridad.

El programa VE sin Filtro ganó el premio Frida por una Internet Libre y Abierta, otorgado por LACNIC. Su trabajo es considerado en los reportes de otras organizaciones de Derechos Humanos y citado por Time, The Washington Post y El País.

La documentación de VE Sin Filtro ha sido fundamental para que organismos internacionales denuncien al Estado venezolano por el uso abusivo de sus potestades, por la aplicación de censura previa contra contenidos de interés público y por la falta de políticas que garanticen un acceso igualitario a internet.

Índice


ERROR
404
451

1 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), Una de las metas es "aumentar significativamente el acceso a Internet y a las tecnologías de la información y comunicación (TICs) 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% 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 de 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.

Las fuentes de información que cubren el acceso a Internet en Venezuela tienden a ofrecer cifras diferentes debido a las distintas metodologías. Por ejemplo, la Comisión Nacional de Telecomunicaciones (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.

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 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 gobierno 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.

1.1 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 en situación de vulnerabilidad como los niños, las mujeres, las minorías (migrantes, indígenas y otros) y las personas de bajos ingresos.

Algunos aspectos técnicos relacionados con la calidad y que tienen un impacto crítico en las actividades 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; la velocidad de subida es a la que los datos se transfieren de un dispositivo a Internet. La velocidad de Internet, también llamada ancho de banda, se divide entre los usuarios de una misma 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 signi-

fica 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.

1.2 Penetración de Internet

Siendo el Internet un mediador esencial para el ejercicio de los derechos humanos hoy en día, su acceso se hace fundamental para participar de manera plena en la sociedad.

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.

Las fuentes oficiales de penetración de Internet provienen de CONATEL, con una metodología que no está suficientemente documentada. CONATEL reporta una penetración de 55.34% al cierre de 2022, un aumento de 1.29 puntos porcentuales en comparación con el último trimestre de 2021. Si se promedian las cifras del año para reducir variaciones entre trimestre, 2022 en promedio tuvo una penetración de Internet 0.72 puntos menor al 2021.

Estas cifras oficiales de penetración de Internet cuentan usuarios que exclusivamente tienen acceso a telefonía móvil y en planes de datos realmente que no son suficientes. Con frecuencia que no funcionan suficientemente bien en sus hogares. Igualmente, parecen asumir que todos los clientes de servicios de Internet tienen una conexión en funcionamiento, pero un gran número de clientes de CANTV no han tenido servicio durante

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

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 por tiempo muy prolongado.

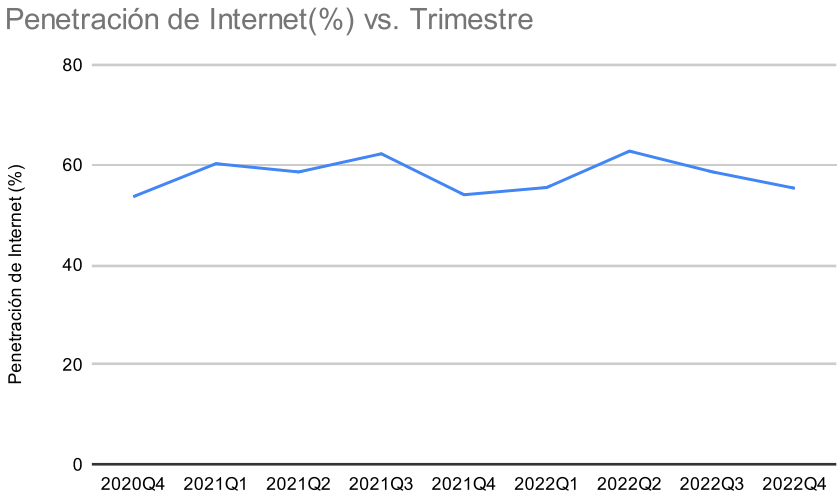


Gráfico de la penetración de Internet en Venezuela por trimestre anual, determinada utilizando las cifras de penetración de Internet de CONATEL.(Fuente: VE sin Filtro vía CONATEL)

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

Tasa de Penetración en Latam 2023

Fuente: Kepios

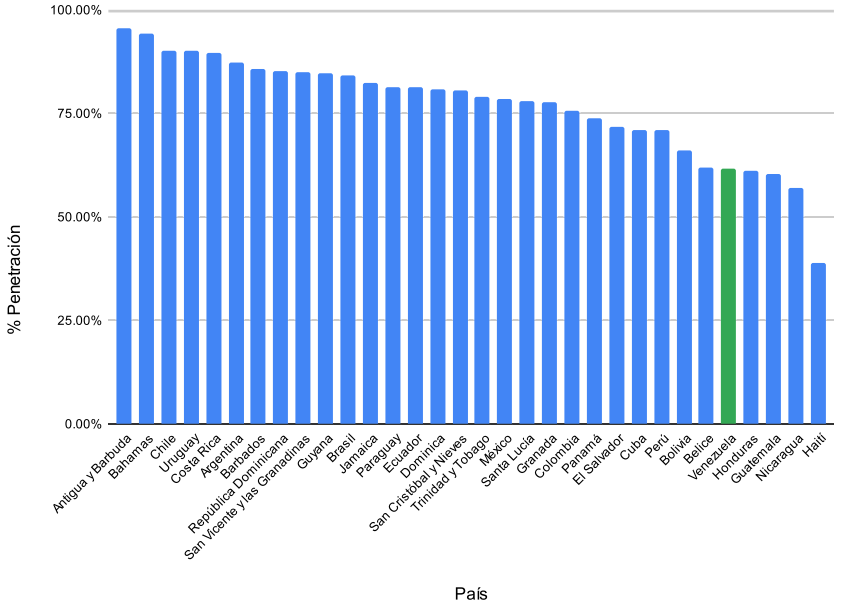


Gráfico de barras que muestra la tasa de penetración en América Latina basada en datos de Kepios de su primera publicación del año 2023. (Fuente: Kepios).

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 Cojedes pasa a ocupar el último puesto de esta lista, mientras que el Distrito Capital y el estado Miranda tienen 167,34% y 90,22% de penetración de Internet respectivamente.

Para finales de 2022, 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 geopolíticos en Caracas, entre el Distrito Capital, el Distrito Metropolitano de Caracas y el estado Miranda.

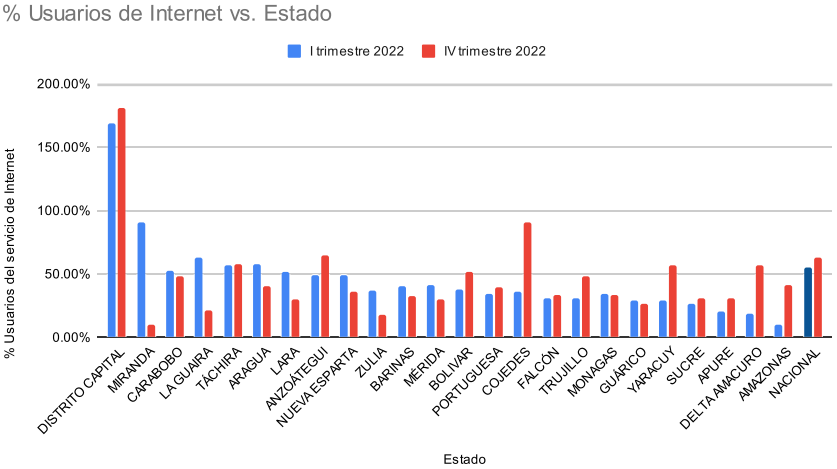


Gráfico de barras del porcentaje de usuarios del servicio de Internet por estado de Venezuela para el 1er y 4to trimestre del año 2022. (Fuente: VE sin Filtro, utilizando datos de CONATEL)

Esto evidencia que hay una brecha importante 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.

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).

1.3 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 para determinar la velocidad de su conexión.

En Venezuela, en enero de 2023 la velocidad mediana de Internet fijo 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. 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 a inicios de 2023.

Velocidad de Internet Fijo (2021-2023)

Fuente: Velocidades de Internet de banda ancha fija en Venezuela - Ookla

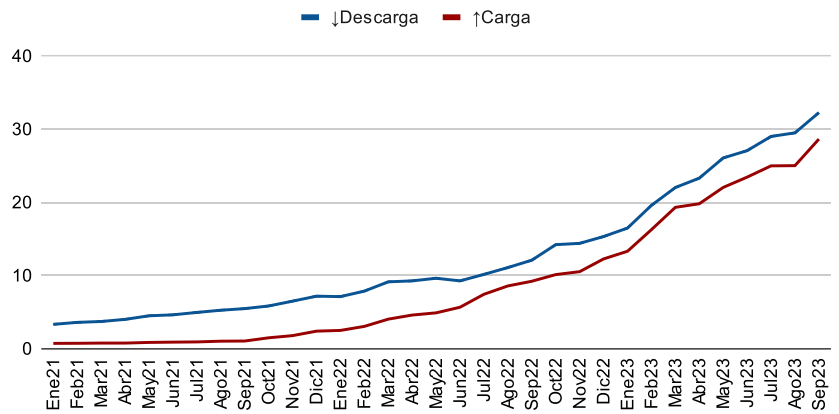


Gráfico de Velocidad de Internet banda ancha fija de carga y descarga desde 2021 al tercer trimestre de 2023. (Fuente: VE sin Filtro, utilizando datos de Ookla).

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%.

Para septiembre de 2023, hubo un aumento de 95.64% con respecto a enero de 2023, teniendo una velocidad mediana de descarga de 32.28 Mbps, mientras que la velocidad de carga es de 28.66 Mbps, lo que significa un aumento de 115% con respecto a la velocidad de carga en enero de 2023, según el Índice Global Speedtest de OOKLA.

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 multi hilo, como el streaming de video. 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.

Densidad de resultados por rango de velocidad de Internet en Venezuela

% de todas las pruebas de Venezuela en 2022. Fuente: Network Diagnostic Tool de M-Lab.

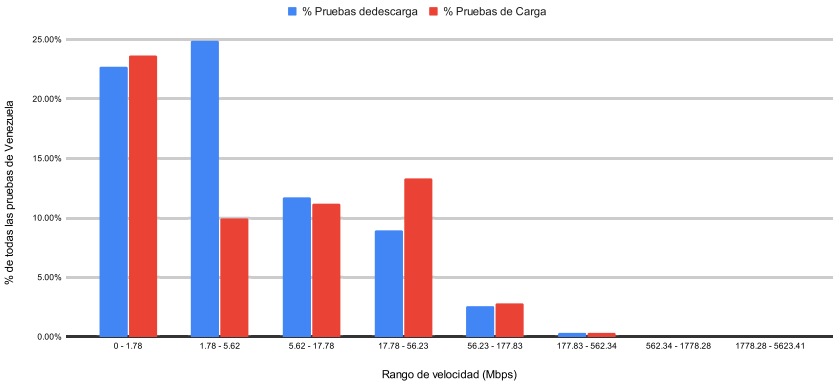


Gráfico de barras de la distribución de los resultados de las pruebas de velocidad en Venezuela por rango de velocidad durante el año natural 2022 utilizando mediciones de Network Diagnostics Tool. (Fuente: VE sin Filtro, utilizando datos de M-Lab).

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 medianas, es importante tener en cuenta que la velocidad mediana 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.

1.4 Oferta

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

Según el análisis realizado por VE sin Filtro de la oferta del servicio de Internet para el primer trimestre de 2023, mediante la investigación de la oferta y precios de los planes de servicio de Internet, 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 Observatorio Social Humanitario de diciembre de 2022[2], 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%.

En cuanto a la velocidad de los planes disponibles, el 60,5% de ellos tiene 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.

1.5 Costo

Un análisis de los paquetes de servicios de 24 ISPs nacionales realizado de enero a marzo de 2023 demuestra el elevado coste de los servicios, lo que es un obstáculo para el acceso a Internet de los venezolanos. **Los 115 planes analizados muestran unos precios que van 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 que cuestan entre 4,44 y 6,93 veces el salario mínimo mensual, lo que representa el 22,6% de los planes analizados. Y

[2] Observatorio Social Humanitario. (2023). Monitoreo Comunitario de Servicos Públicos. Reporte 4: Evaluación de la existencia, calidad y desempeño de los servicios públicos en Venezuela. Observatorio Social Humanitario.

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 perciben el salario mínimo mensual o un poco más.

Oferta de Planes de Servicio de Internet

Fuente: Ve Sin Filtro

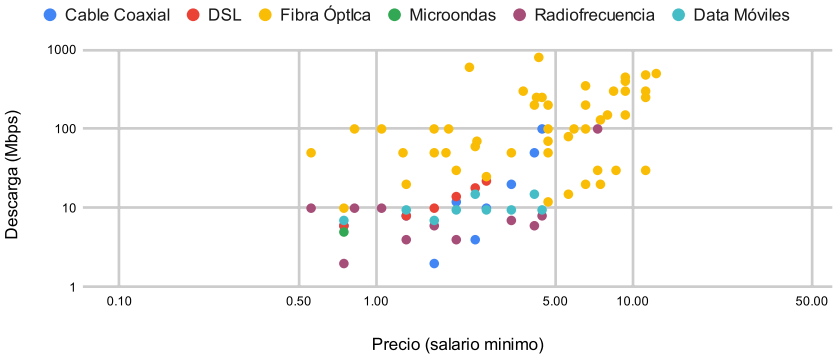


Gráfico de dispersión de los planes de servicio de Internet en Venezuela por velocidad de descarga y precio en función del salario mínimo mensual venezolano de 2022. (Fuente: VE sin Filtro)

La inflación que ha experimentado Venezuela en los últimos años ha disminuido significativamente el poder adquisitivo de una buena parte de los 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 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.

1.6 Distribución Geográfica

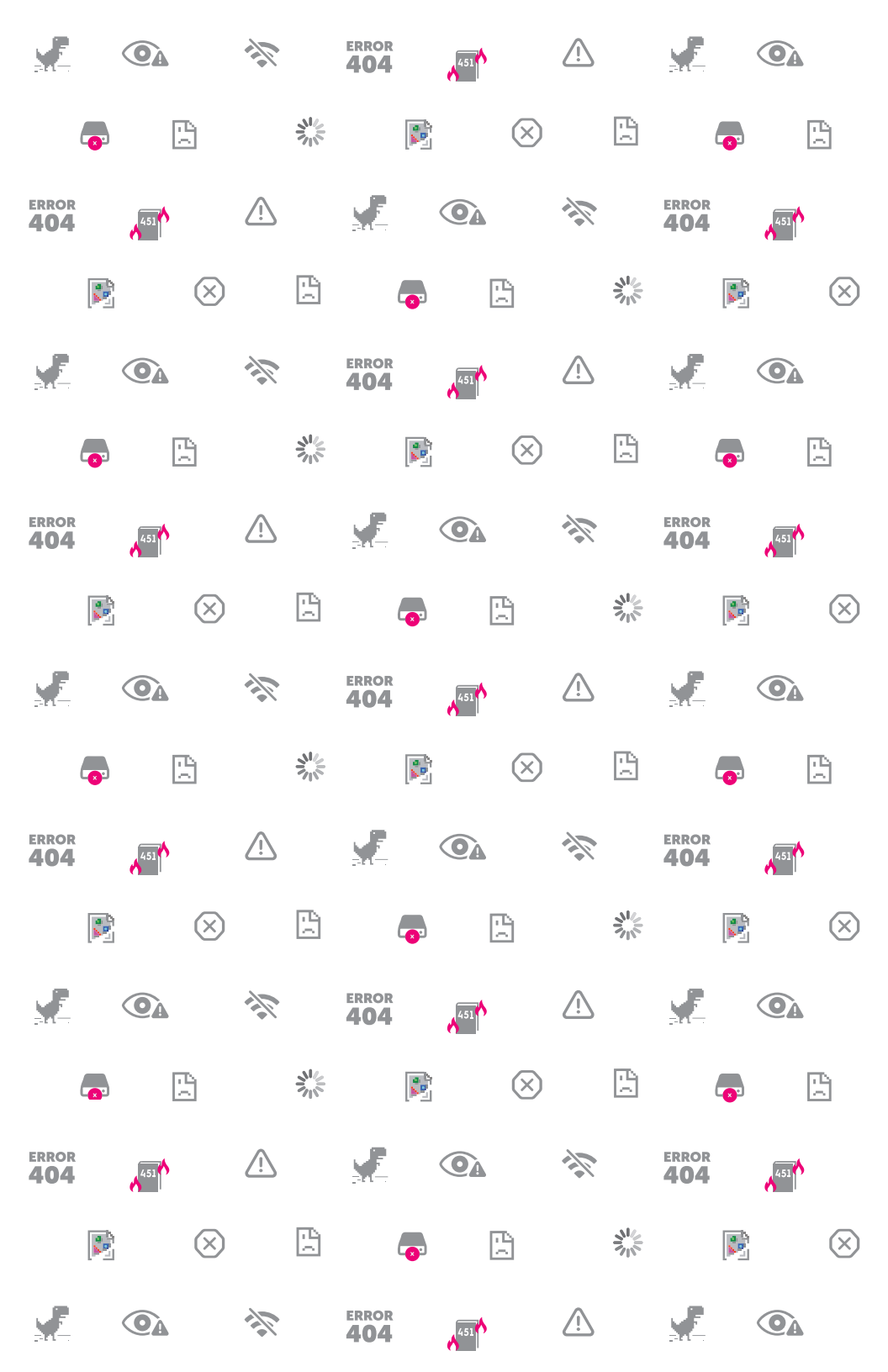
En cuanto a la distribución geográfica de la oferta del servicio de Internet, es relevante la desigual distribución en los distintos estados y otros territorios del país: mientras que la mitad de los ISP ofrecen servicios en Caracas, la mayoría de los lugares no tienen muchas opciones, si es que tienen 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 pene-

tración, 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 la Cámara de Empresas de Servicios de Telecomunicaciones (Casetel) , Pedro Marín, ha explicado que una de las razones por las que la mayoría de los ISP dan servicio sólo a unas pocas ciudades importantes[3], principalmente Caracas, Maracaibo, Barquisimeto y Valencia, es el alto costo 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.

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


ERROR
404
451

2 CENSURA MEDIANTE BLOQUEOS EN INTERNET

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 el ejercicio de 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.

Eventos de bloqueo:
Los bloqueos son documentados principalmente como eventos, para evitar la ambigüedad que puede existir cuando distintas acciones de bloqueo afectan a un mismo servicio en Internet. El término evento de bloqueo hace referencia al bloqueo de una URL, dominio o dirección IP, utilizando una técnica de bloqueo específica y por un ISP en particular.

Por ejemplo: el URL "caraotadigital.xyz" perteneciente al sito web del medio de noticias Caraota Digital, presenta 7 eventos de bloqueos, estos son 6 bloqueos de tipo DNS en los ISPs CANTV, Digitel, Movistar, Inter, Net Uno y Supercable, y un bloqueo de tipo HTTP en CANTV, por lo que se registró un total de 7 eventos de bloqueo en un mismo **caso.**

Casos de Bloqueo:
Alternativamente, todos los eventos de bloqueo contra un mismo servicio o sitio web se consideran un caso, que agrupa a los eventos de bloqueos de distintos dominios. Es decir, cada forma de censura implementada por los distintos ISP.

La mayoría de los bloqueos documentados son de tipo DNS. Con este tipo de bloqueo los ISP reconfiguran sus servidores de servicio de nombres de directorio (por sus siglas en inglés DNS: directory name service), que convierten los nombres de dominio en direcciones de Internet (direcciones IP), haciendo que respondan incorrectamente a las solicitudes de los dominios de los sitios web u otros servicios en línea que desea bloquear. Esta práctica es relativamente sencilla y no representa ningún costo para los operadores de Internet que las ejecutan.

Mientras tanto, **los bloqueos HTTP y HTTPS afectan al contenido de las conexiones a Internet en múltiples capas del proceso, con equipos especialmente diseñados para examinar cada comunicación** en busca de

elementos específicos en los paquetes de Internet, como el nombre de host del sitio web, la URL solicitada, las palabras claves en el cuerpo del sitio web o la Indicación de Nombre de Servidor (SNI) para verificar si debe bloquearse en lo que se denomina "Inspección Profunda de Paquetes" (DPI, por sus siglas en inglés). Como consecuencia, el bloqueo HTTP/HTTPS aplicado por la estatal CANTV, por ejemplo, obliga al usuario a utilizar una VPN para eludir la censura.

2.1 Bloqueos en 2022

VE sin Filtro identificó en 2022 más de 108 URLs 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	21
Economics	ECON	2	4	25
Hate Speech	HATE	1	1	6
Human Rights Issues	HUMR	4	4	16
Media Sharing	MMED	3	3	16
News Media	NEWS	43	66	336
Political Criticism	POLR	12	12	54
Pornography	PORN	8	8	21
Public Health	PUBH	2	2	8
Anonymization and circumvention tools	VPN	3	5	26
TOTAL AÑO 2022		77	108	529

Tabla con el número de casos sitios web bloqueados, urls o dominios bloqueados y eventos de bloqueo por categoría registrados en 2022.

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 empresas públicas como privadas: CANTV, Movistar, Inter, Digitel, Net Uno y Supercable, estos son los proveedores con mayor porcentaje de distribución del mercado según Conatel[4][5][6][7].

[4] Conatel. INFORME DE LAS CIFRAS DEL SECTOR Telecomunicaciones I TRIMESTRE 2022 (segunda versión publicada)
[5] Conatel. INFORME DE LAS CIFRAS DEL SECTOR Telecomunicaciones II TRIMESTRE 2022
[6] Conatel. INFORME DE LAS CIFRAS DEL SECTOR Telecomunicaciones III TRIMESTRE 2022
[7] Conatel. INFORME DE LAS CIFRAS DEL SECTOR Telecomunicaciones IV TRIMESTRE 2022

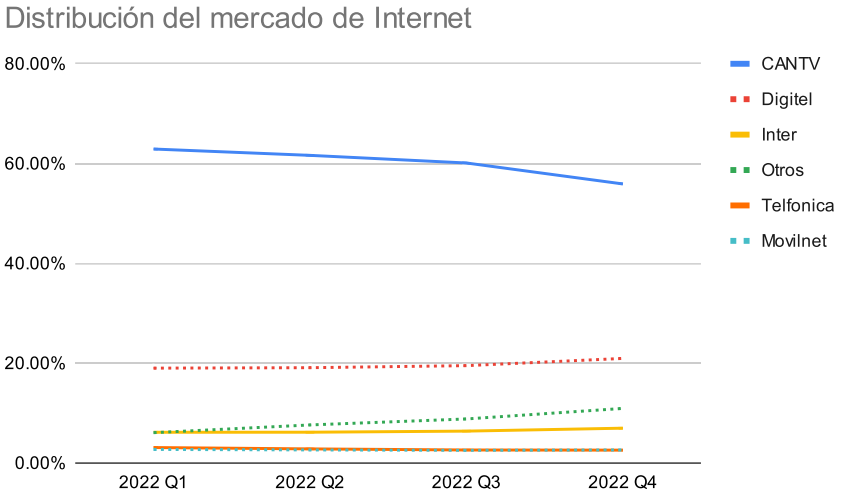


Gráfico de la distribución de mercado de internet tradiconal en Venezuela durante el año 2022, determinada utilizando las cifras de penetración de Internet de CONATEL. (Fuente: VE sin Filtro vía CONATEL)

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, la participación política y el desarrollo de actividades laborales entre muchas otras.

Los bloqueos de sitios web en Venezuela no se ajustan a las normas internacionales de derechos humanos. Se ordenan de oficio, a discreción de 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 no son supervisadas o dictadas por un juez.

2.2 Medios de Comunicación

SITIO	DOMINIO	CATEGORIA	CANTV	Movistar	Digitel	Inter	NetUno	Super Cable
2001	www.2001.com.ve	NEWS	HTTP+DNS	No	No	No	No	No
6to poder	6topoder.com	NEWS	DNS	DNS	DNS	DNS	DNS	DNS
Aguacateverde.com	www.aguacateverde.com	NEWS	HTTP+DNS	DNS	DNS	No	DNS	DNS
Al navio	alnavio.com	NEWS	HTTP+DNS	DNS	DNS	DNS	DNS	DNS
Alberto News	albertonews.com	NEWS	HTTP+DNS	DNS	DNS	DNS	DNS	No
Alberto News	awsveanews.com	NEWS	HTTP	No	No	No	No	No
Alberto News	b1tly4n3s.com	NEWS	HTTP	No	No	No	No	No
Alberto News	www.b1tlydns02io.com	NEWS	HTTP	No	No	No	No	No
Alek boyd	alekboyd.blogspot.co.uk	NEWS	HTTP+DNS	DNS	DNS	No	DNS	DNS
Alek boyd	alekboyd.blogspot.com	NEWS	No	DNS	DNS	No	DNS	DNS
Analisis 24	analisis24.com	NEWS	No	DNS	No	DNS	DNS	No
Antena 3	antena3internacional.com	NEWS	HTTP+DNS	No	No	No	No	No
Aporrea	www.aporrea.org	NEWS	HTTP	No	No	No	No	No
Armando info	armando.info	NEWS	HTTP+DNS	DNS	DNS	DNS	No	DNS
Caraota digital	caraotadigital.news	NEWS	HTTP+DNS	DNS	DNS	DNS	DNS	DNS
Caraota digital	caraotadigital.xyz	NEWS	HTTP+DNS	DNS	DNS	DNS	DNS	DNS
Caraota digital	www.adncaraota.com	NEWS	HTTP	No	No	No	No	No
Caraota digital	www.caraotadigital.net	NEWS	HTTP+DNS	DNS	DNS	DNS	DNS	DNS
Cronica Uno	cronica.uno	NEWS	HTTP+DNS	DNS	DNS	DNS	DNS	DNS
Diario La region	diariolaregion.net	NEWS	HTTP+DNS	DNS	No	DNS	DNS	DNS
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
Dolar today	bit.ly	NEWS	No	HTTP	No	No	No	No
Dolar today	dolartoday.com	NEWS	HTTP	DNS	DNS	DNS	DNS	DNS
Dolar today	dolartoday.info	NEWS	HTTP+DNS	DNS	DNS	DNS	DNS	DNS

SITIO	DOMINIO	CATEGORIA	CANTV	Movistar	Digitel	Inter	NetUno	Super Cable
Dolar today	dolartoday.org	NEWS	HTTP+DNS	DNS	DNS	DNS	DNS	DNS
Dollar.nu	dollar.nu	NEWS	HTTP+DNS	DNS	DNS	DNS	DNS	DNS
Efecto cocuyo	efectococuyo.com	NEWS	HTTP+DNS	DNS	DNS	DNS	DNS	DNS
El diario	eldiario.com	NEWS	HTTP	No	No	No	No	No
El Liberal Venezolano	liberal-venezolano.blogspot.com	NEWS	HTTP+DNS	DNS	DNS	DNS	DNS	DNS
El Nacional	www.el-nacional.com	NEWS	HTTP+DNS	DNS	DNS	DNS	DNS	DNS
El Nacional	www.elnacional.com	NEWS	HTTP+DNS	DNS	DNS	DNS	DNS	DNS
El Pitazo	elpitazo.com	NEWS	HTTP+DNS	DNS	DNS	No	DNS	DNS
El Pitazo	elpitazo.info	NEWS	HTTP+DNS	DNS	DNS	No	DNS	DNS
El Pitazo	elpitazo.net	NEWS	HTTP+DNS	DNS	DNS	DNS	DNS	DNS
El tiempo	www.eltiempo.com	NEWS	HTTP+DNS	DNS	DNS	DNS	DNS	DNS
eldolarparalelo.info	eldolarparalelo.info	NEWS	HTTP+DNS	DNS	DNS	DNS	DNS	DNS
EVTV	evtv.online	NEWS	HTTP+DNS	DNS	DNS	DNS	DNS	DNS
EVTV	evtvmiami.com	NEWS	HTTP	DNS	DNS	DNS	DNS	No
Infobae	infob.ae	NEWS	HTTP	DNS	DNS	HTTP	DNS	No
Infobae	www.infobae.com	NEWS	HTTP+DNS	DNS	DNS	DNS	DNS	DNS
Infobae	www.infobae.media	NEWS	HTTP+DNS	DNS	DNS	DNS	DNS	DNS
Insight Crime	es.insightcrime.org	NEWS	HTTP	No	No	No	No	No
Insight Crime	www.insightcrime.org	NEWS	HTTP	No	No	No	No	No
La manada digital	lamananadigital.com	NEWS	HTTP+DNS	No	No	No	No	No
La patilla	lapatilla.com	NEWS	HTTP+DNS	DNS	DNS	DNS	DNS	DNS
La patilla	www.lapatilla.com	NEWS	HTTP+DNS	DNS	DNS	DNS	DNS	DNS
Maduradas	maduradas.com	NEWS	HTTP+DNS	DNS	DNS	No	DNS	No
Minuto 30	minuto30.com	NEWS	HTTP+DNS	DNS	DNS	DNS	DNS	DNS
Monitoreamos	monitoreamos.com	NEWS	HTTP	DNS	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	DNS

SITIO	DOMINIO	CATEGORIA	CANTV	Movistar	Digitel	Inter	NetUno	Super Cable
Noticias venezuela	noticiasvenezuela.org	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
Primer Informe	primerinforme.com	NEWS	HTTP+DNS	DNS	No	DNS	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
Sumarium	sumarium.es	NEWS	HTTP+DNS	No	No	No	No	No
TV Venezuela	www.tvvenezuela.tv	NEWS	HTTP+DNS	DNS	DNS	DNS	DNS	DNS
Venezuela al dia	venezuelaaldia.com	NEWS	No	DNS	No	DNS	DNS	No
Venezuela al dia	www.venezuelaaldia.com	NEWS	No	DNS	DNS	DNS	DNS	No
Vivo play	vivoplay.net	NEWS	HTTP	DNS	DNS	No	DNS	No
VPITV	vpitv.com	NEWS	HTTP+DNS	No	DNS	DNS	DNS	DNS
VPITV	www.vpitv.com	NEWS	HTTP+DNS	DNS	DNS	DNS	DNS	DNS
Soundcloud	soundcloud.com	MMED	HTTP+DNS	DNS	DNS	No	DNS	DNS
LiveStream	livestream.com	MMED	DNS	No	DNS	DNS	DNS	DNS
Reddit	www.reddit.com	MMED	No	DNS	No	No	No	No
Zello	zello.com	MMED	DNS	HTTP	DNS	No	No	No

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

2.3 Sociedad civil, activismo y 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	Movistar	Digitel	Inter	NetUno	Super Cable
Mi Convive	miconvive.com	HUMR	HTTP+DNS	DNS	DNS	DNS	DNS	DNS
Acceso a la Justicia	accesoalajusticia.org	HUMR	HTTP	No	No	No	No	No
Change.org	www.change.org	HUMR	HTTP+DNS	DNS	DNS	DNS	DNS	DNS
Justicia, Encuentro y Perdón	www.jepvenezuela.com	HUMR	HTTP	No	No	No	No	No

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

VE sin Filtro determinó que el sitio web www.jepvenezuela.com, perteneciente a la ONG Justicia, Encuentro, y Perdón (JEP), se encuentra actualmente bloqueado. Esta organización ha monitoreado y documentado violaciones a los derechos humanos desde 2017, a menudo tomando acciones ante organismos nacionales e internacionales, como un medio para asegurar justicia, protección y reparación para las víctimas de esas violaciones. La organización representa a víctimas de asesinatos y detenciones entre 2014 y 2017. La ONG también informa sobre los actos de tortura contra 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 VE sin Filtro también encontró que el ISP Movistar mantiene un bloqueo HTTP.

La plataforma de incidencia Change.org continuó estando bloqueada, VE sin Filtro confirmó que fue bloqueada inicialmente por CANTV en febrero de 2019, pocos días después de que varios medios de comunicación fueran bloqueados por cubrir un evento en el que participó Juan Guaidó. El evento, que pretendía movilizar apoyo y facilitar la llegada de ayuda humanitaria, incluyó un concierto con artistas latinoamericanos en la frontera con Colombia.

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. Por su parte, JEP Venezuela promueve el acceso a la justicia en el país.

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.

2.4 Herramientas de evasión de censura

El gobierno de Venezuela está bloqueando el acceso a herramientas de evasión de 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.

El bloqueo a las páginas web de las VPN TunnelBear y Psiphon continuó durante 2022 y 2023 en los principales ISP, incluido CANTV. El bloqueo de TunnelBear es más completo, ya que no solo afecta el acceso a su página web, sino que también intenta, sin éxito, impedir el funcionamiento de la VPN.

En CANTV el bloqueo es de tipo 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, VPN y otras herramientas, de ser más efectivos, tendrían un gravísimo impacto en la capacidad de los venezolanos para acceder a información en línea que de otro modo estaría restringida.

SITIO	DOMINIO	CATEGORIA	CANTV	Movistar	Digitel	Inter	NetUno	Super Cable
Hidemyass	www.hidemyass.com	VPN	No	No	No	No	DNS	No
Psiphon	psiphon.ca	VPN	HTTP+DNS	DNS	No	DNS	DNS	DNS
Tunnelbear	api.tunnelbear.com	VPN	HTTP+DNS	DNS	No	No	DNS	DNS
Tunnelbear	tunnelbear.com	VPN	HTTP+DNS	DNS	No	HTTP+DNS	DNS	DNS
Tunnelbear	tunnelbear.com	VPN	HTTP+DNS	DNS	DNS	DNS	DNS	DNS

Tabla que muestra los bloqueos activos de dominios de herramientas de evasión de censura, durante 2022.

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 las comunicaciones con su servidor mediante su API (nterfaz de programación de aplicaciones, 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 su funcionamiento, permitiendo así a los usuarios venezolanos acceder de nuevo a una VPN plenamente 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.

2.5 Bloqueos adicionales de enero a octubre de 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. Esto ocurrió durante un intenso período de protestas sindicales.

En el primer semestre de 2023 el Observatorio Venezolano de Conflictividad Social (OVCS) registró 3754 protestas exigiendo Derechos Económicos, Sociales, Culturales y Ambientales, el 86% de todas las manifestaciones que registraron en ese período.

Este bloqueo está activo en CANTV, Digitel e Inter de tipo DNS y Movistar lo hizo aplicando un bloqueo HTTPS/HTTP, lo cual es es poco característico ya que suelen aplicar un bloqueo DNS.

La página del Observatorio de Finanzas se encuentra bloqueada desde el 3 de mayo por CANTV, Movistar, Digitel, Supercable e Inter. Este bloqueo censuró una fuente independiente de información y análisis de la inflación y actividad económica en Venezuela, frente a la ausencia de datos oficiales y en un momento de conflictividad social relacionada a los salarios y exigencias laborales. En Movistar la modalidad del bloqueo es HTTPS/HTTP + DNS, mientras que los otros 3 proveedores aplicaron solo bloqueo DNS.

Varios sitios web de noticias también fueron bloqueados desde enero hasta octubre de 2023, sumándose a la ya generalizada censura de fuentes de noticias independientes en el país. Noticias.com fue bloqueada en todos los principales ISP analizados. Los dominios focoinformativo.com y opinionynoticias.com se encuentran bloqueados únicamente en movistar, en el primer dominio el bloqueo es de tipo HTTPS/HTTP+DNS y de tipo HTTPS/HTTP en el segundo caso. Estos 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	Movistar	Digitel	Inter	NetUno	Super Cable
El Diario	eldiario.com	NEWS	HTTPS+DNS	No	No	No	No	No
Salario Digno VZLA	salariodignovzla.com	HUMR	DNS	HTTPS/HTTP	DNS	DNS	No	No
Observatorio de Finanzas	observatoriodefinanzas.com	HUMR	DNS	HTTPS/ HTTP+DNS	DNS	DNS	No	DNS
Foco Informativo	focoinformativo.com	NEWS	No	HTTPS/ HTTP+DNS	No	No	No	No
Opinion y Noticias	www.opinionynoticias.com	NEWS	No	HTTPS/HTTP	No	No	No	No
Noticias del Mundo	noticias.com	NEWS	DNS	HTTPS/ HTTP+DNS	DNS	DNS	DNS	DNS

Tabla que muestra los bloqueos de páginas iniciados en el primer semestre de 2023, según lo registrado por VE sin Filtro.

2.6 Bloqueos durante la primaria de oposición

VE sin Filtro documentó bloqueos contra la infraestructura habilitada por la Comisión Nacional de Primaria, principalmente contra los sitios de buscadores de centros de votación y la página de la Comisión. En el pasado hemos documentado bloqueos y otras formas de interferencia utilizando la tecnología digital, para impedir la participación y la expresión de las voces disidentes. Estas prácticas atentan contra el espacio cívico y niegan el derecho a la libre asociación

A partir del 7 de septiembre, a más de un mes para las elecciones que se celebraron el 22 de octubre, se encontró activo un bloqueo de tipo DNS en Digitel, Inter, Supercable y la estatal CANTV. Movistar aplicó un bloqueo tipo HTTPS/HTTP.

Luego, dos dominios creados para el mismo fin fueron bloqueados también y desde el 14 de octubre aplicaron las mismas restricciones a la página principal de la Comisión.

SITIO	DOMINIO	CATEGORIA	CANTV	Movistar	Digitel	Inter	NetUno	Super Cable
Buscador primarias 2023	buscadorprimaria2023.com	POLR	DNS	HTTPS/HTTP	DNS	DNS	DNS	DNS
Buscador primarias 2023	d1zjwmfds04x7i.cloudfront.net	POLR	DNS	DNS	DNS	DNS	No	No
Buscador primarias 2023	d3lokqj5h9z9zs.cloudfront.net	POLR	DNS	DNS	DNS	No	No	No
Comison primarias	comisiondeprimariave.org	POLR	DNS	DNS	DNS	No	No	No
la venezuela del encuentro	lavenezueladelencuentro.com	POLR	DNS	DNS	DNS	No	No	No

Tabla de los dominios bloqueados relacionados con la primaria de Octubre 2023, según documentado por VE sin Filtro

De manera independiente, VE sin Filtro no pudo confirmar el bloqueo a los servidores de transmisión de resultados, como lo denunció la Comisión Nacional de Primaria, sin embargo, hay antecedentes similares como el

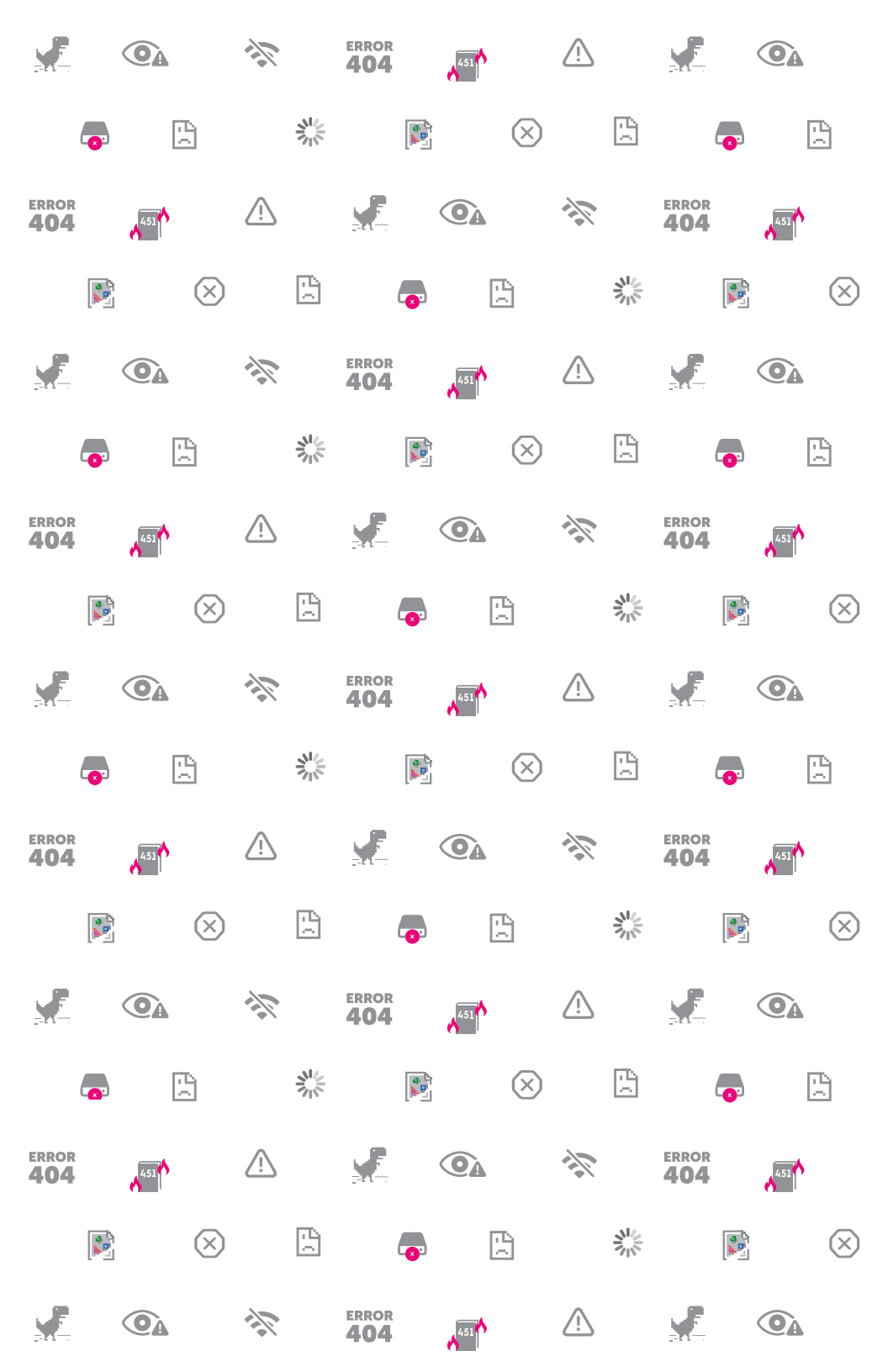
bloqueo de CANTV a servidores de la aplicación Voatz, uno de los canales de participación en la Consulta Popular de 2020.

El uso de la censura en Internet para coartar la participación ciudadana en un evento de esta naturaleza es un severo ataque a los derechos civiles y políticos, la libertad de participación, de asociación y los derechos a elegir y a ser elegidos.

Incluyendo los bloqueos a sitios relacionados con la elección primaria de oposición, de enero a octubre de 2023 117 dominios estuvieron bloqueados, incluyendo 16 dominios relacionados con crítica política y movimientos de oposición, un aumento de 45% sobre los dominios que estuvieron bloqueados en 2022.

CATEGORÍA	ABREVIATURA	CASOS DE SITIOS WEB BLOQUEADOS	URLS O DOMINIOS BLOQUEADOS	TOTAL DE EVENTOS DE BLOQUEO
E-commerce	COMM	1	4	23
Economics	ECON	2	4	22
Hate Speech	HATE	2	2	9
Human Rights Issues	HUMR	5	6	26
Media Sharing	MMED	3	3	13
News Media	NEWS	48	73	342
Political Criticism	POLR	14	16	70
Pornography	PORN	2	2	2
Public Health	PUBH	2	2	8
Anonymization and circumvention tools	VPN	3	5	26
TOTAL AÑO 2022		80	117	541

Tabla con el número de casos de sitios web bloqueados, urls o dominios bloqueados y eventos de bloqueo por categoría registrados de enero a octubre de 2023.


ERROR
404
451

3 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 donde cae la conectividad a Internet, 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.

Incidente:
Caída de conectividad a nivel nacional.

Eventos:
Reflejo de la caída de conectividad nacional en estados o Isps en particular.

Los incidentes se clasifican en función de su nivel de gravedad (crítico, grave o leve) y de su origen, como un apagón, falla del ISP, o cortes intencionados de Internet. 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/o 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.

Los proveedores de Internet monitoreados con mayor detalle por VE sin Filtro son: CANTV, Digitel, Movistar, Intercable, Net Uno y supercable, como se mencionó previamente estos proveedores son los que tienen el mayor porcentaje de participación en el mercado, según CONATEL[8][9][10][11].

[8] Conatel. INFORME DE LAS CIFRAS DEL SECTOR Telecomunicaciones I TRIMESTRE 2022
[9] Conatel. INFORME DE LAS CIFRAS DEL SECTOR Telecomunicaciones II TRIMESTRE 2022
[10] Conatel. INFORME DE LAS CIFRAS DEL SECTOR Telecomunicaciones III TRIMESTRE 2022
[11] Conatel. INFORME DE LAS CIFRAS DEL SECTOR Telecomunicaciones IV TRIMESTRE 2022

3.1 Incidentes de Conectividad

En 2022, VE sin Filtro registró un total de 86 interrupciones de la conectividad a Internet, lo que evidencia un aumento del 83% de los incidentes registrados durante 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.

En agosto de 2022 hubo 12 incidentes, 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.

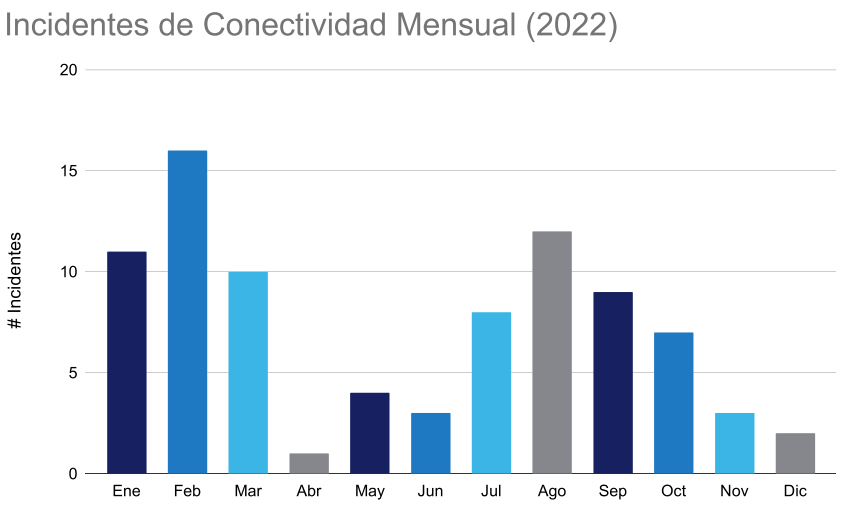


Gráfico de barras que muestra el número de incidentes de conectividad mensualmente de 2022.

En 2022 hubo 474 eventos regionales. Táchira fue 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[12] del OSVP revela que 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.

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

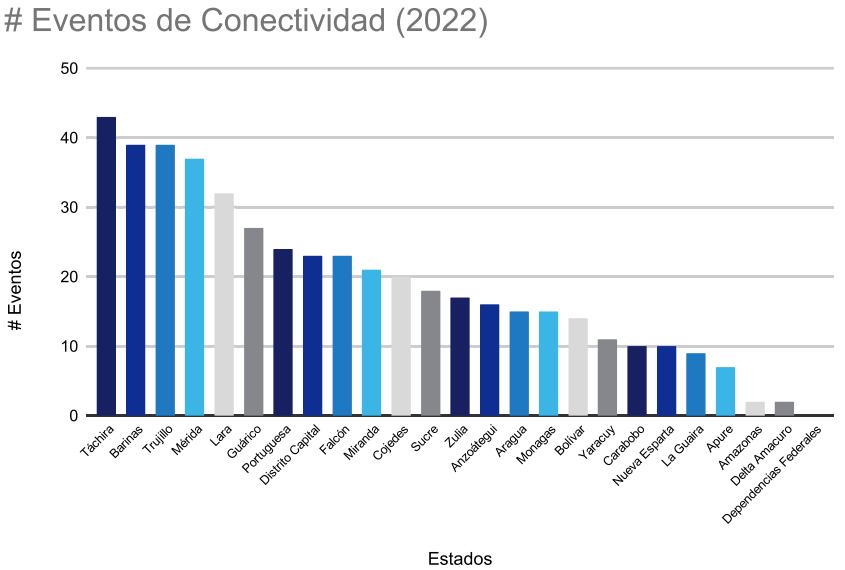


Gráfico de barras que muestra el número de incidentes de conectividad por estado de 2022.

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). Fueron seguidos 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 serios en 2022 con un total de 21, luego le sigue Trujillo con 16 eventos serios, y después están Guárico y Lara con 14 eventos serios ambos estados. Con respecto a los eventos leves en Distrito Capital se registraron 19 eventos en 2022, 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.

Dado que los estados Amazonas, Apure y Delta Amacuro, mayoritariamente rurales, y las Dependencias Federales, tienen los índices de penetra-

ción más bajos, detectar y medir las caídas de 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	CRÍTICO	SERIO	LEVE	# EVENTOS 2022
Táchira	21	11	11	43
Trujillo	19	6	12	37
Barinas	12	1	2	15
Mérida	11	1	2	14
Lara	9	21	9	39
Distrito Capital	7	10	6	23
Falcón	6	16	17	39
Portuguesa	5	5	8	18
Cojedes	4	8	12	24
Guárico	4	5	11	20
Zulia	4	2	1	7
Sucre	2	14	11	27
Miranda	2	6	2	10
Monagas	2	4	4	10
Anzoátegui	2	0	0	2
Bolívar	1	14	17	32
Nueva Esparta	1	12	4	17
Carabobo	1	6	8	15
Aragua	1	4	11	16
La Guaira	1	3	19	23
Yaracuy	1	1	0	2
Apure	0	6	15	21
Delta Amacuro	0	6	5	11
Amazonas	0	5	4	9
Dependencias Federales	0	0	0	0

Tabla que muestra el número de incidencias de interrupción de la conectividad por estado y nivel de gravedad de 2022.

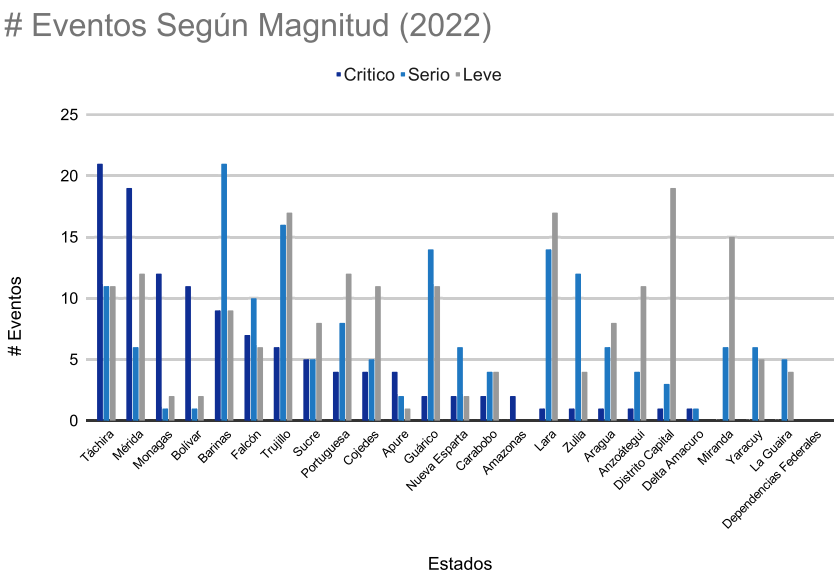


Gráfico de barras que muestra el número de eventos de conectividad por tipo (corte eléctrico, originado por el ISP u otro) de interrupción por estado o distrito venezolano de 2022.

3.2 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.

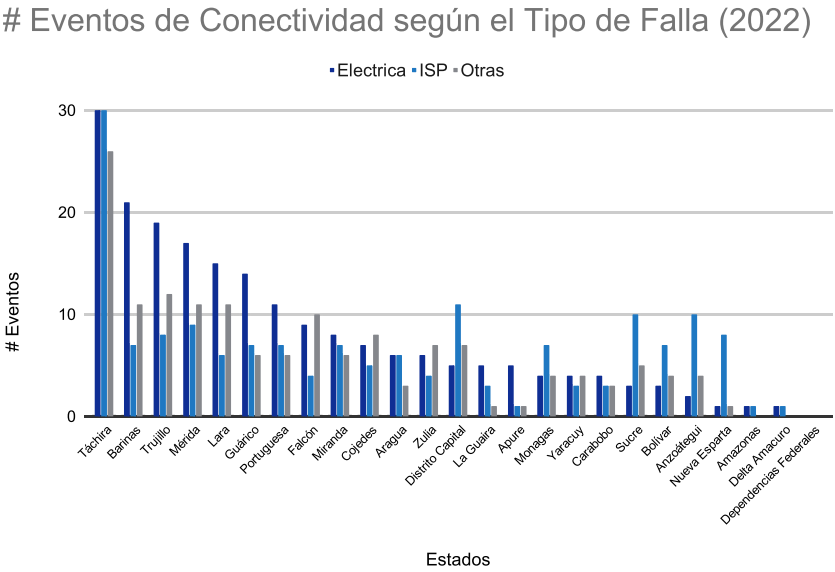


Gráfico de barras que muestra el número de eventos de conectividad por tipo (corte eléctrico, originado por el ISP u otro) de interrupción por estado o distrito venezolano 2022.

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.

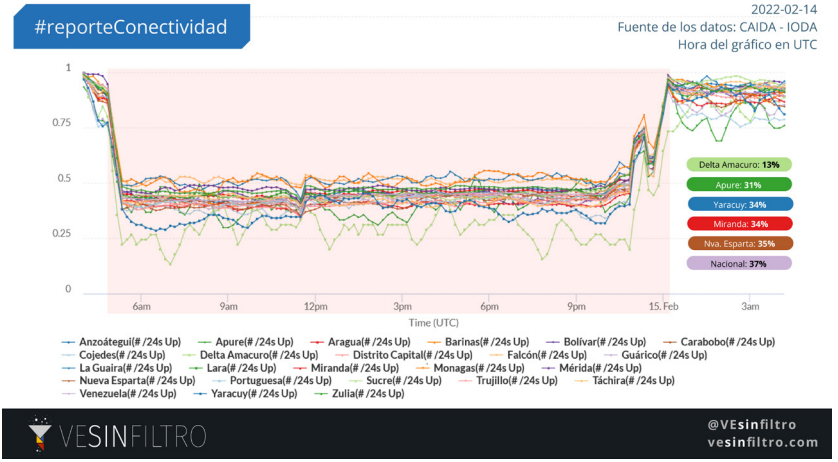


Gráfico lineal compartido en redes sociales que muestra la caída en la conectividad de la mayoría de los estados de Venezuela el 14 de febrero de 2022. Esta señal de conectividad es el número de segmentos IP /24 accesibles mediante sondeo activo, normalizado. (Fuente: VE sin Filtro, con datos obtenidos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

En 2022, el 34,88% de los incidentes fueron de este tipo, es decir, 30 en total. 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 o de origen desconocido, representaron 30,23% del total. 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.

3.3 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.

DURACION DE EVENTOS DE CONECTIVIDAD (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
NACIONAL	**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.

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

3.4 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.

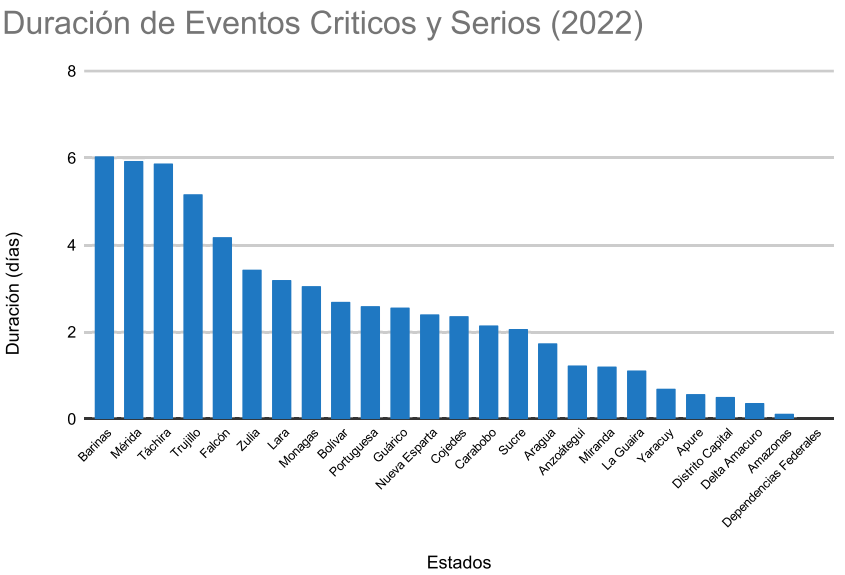


Gráfico de barras que muestra la duración (en días) de los eventos de conectividad por estado, de magnitud crítica y seria, 2022.

3.5 Incidentes por falla de Isp y según la magnitud

La duración total de los eventos por falla de los ISP mostró que los 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 15 eventos en 2022. Duraron un día y siete horas en 2021 y tres días y trece horas en 2022.

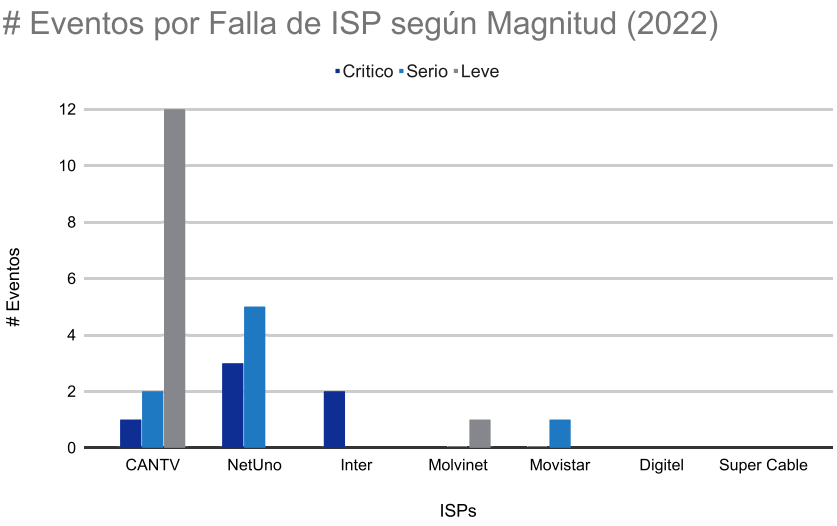


Gráfico de barras que muestra el número de eventos debidos a fallos del ISP por proveedor de 2022.

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)

3.6 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.

Duración de Eventos por Falla de ISP (2022)

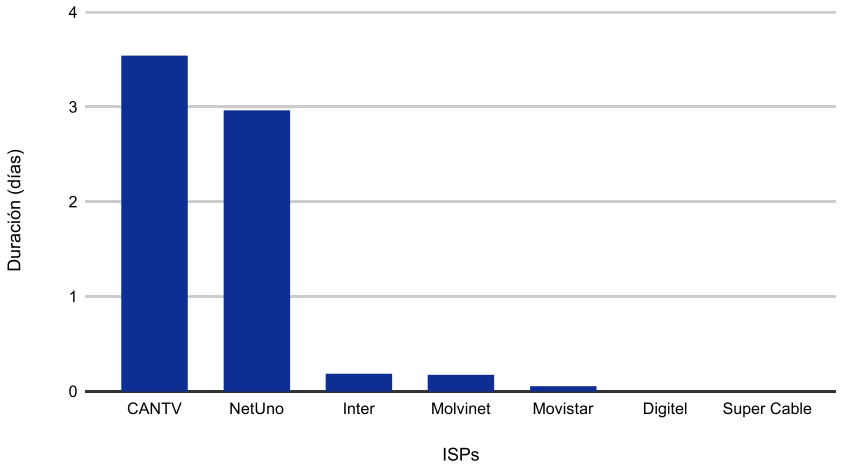


Gráfico de barras que muestra la duración, en días, de los eventos de fallo del ISP por proveedor de 2022.

3.7 Incidentes en el primer semestre de 2023

Incidentes de Conectividad Mensual (1er semestre 2023)

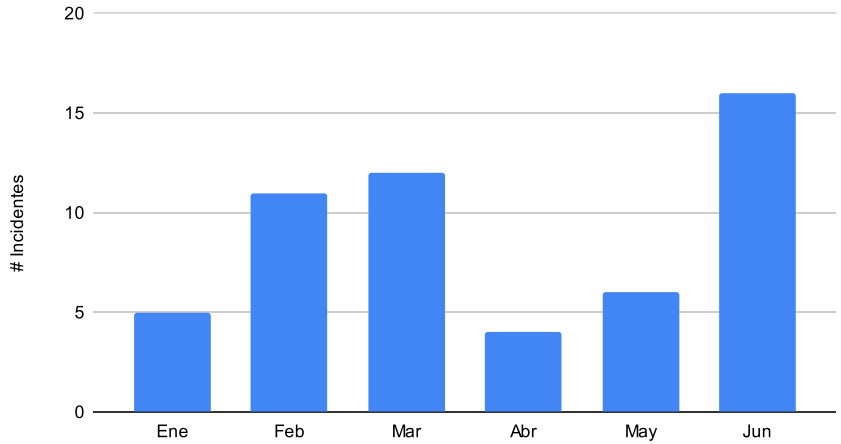


Gráfico de barras que muestra el número de incidentes de conectividad mensualmente durante el primer semestre de 2023, documentado por VE Sin Filtro.

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. Esto representa el 62,79% de los incidentes totales ocurridos durante 2022. En junio de 2023 hubo 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 los cuales afectaron al 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.

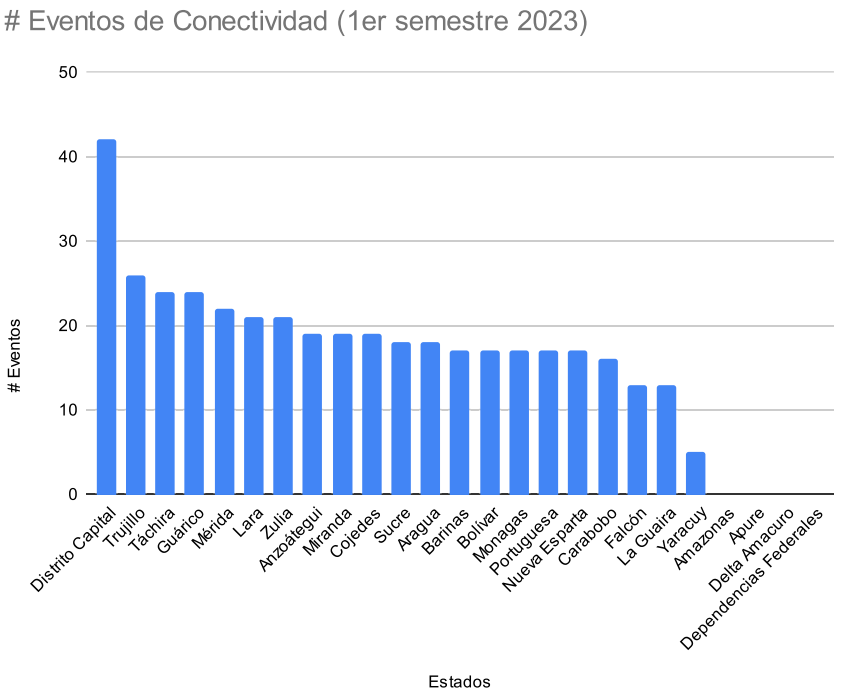
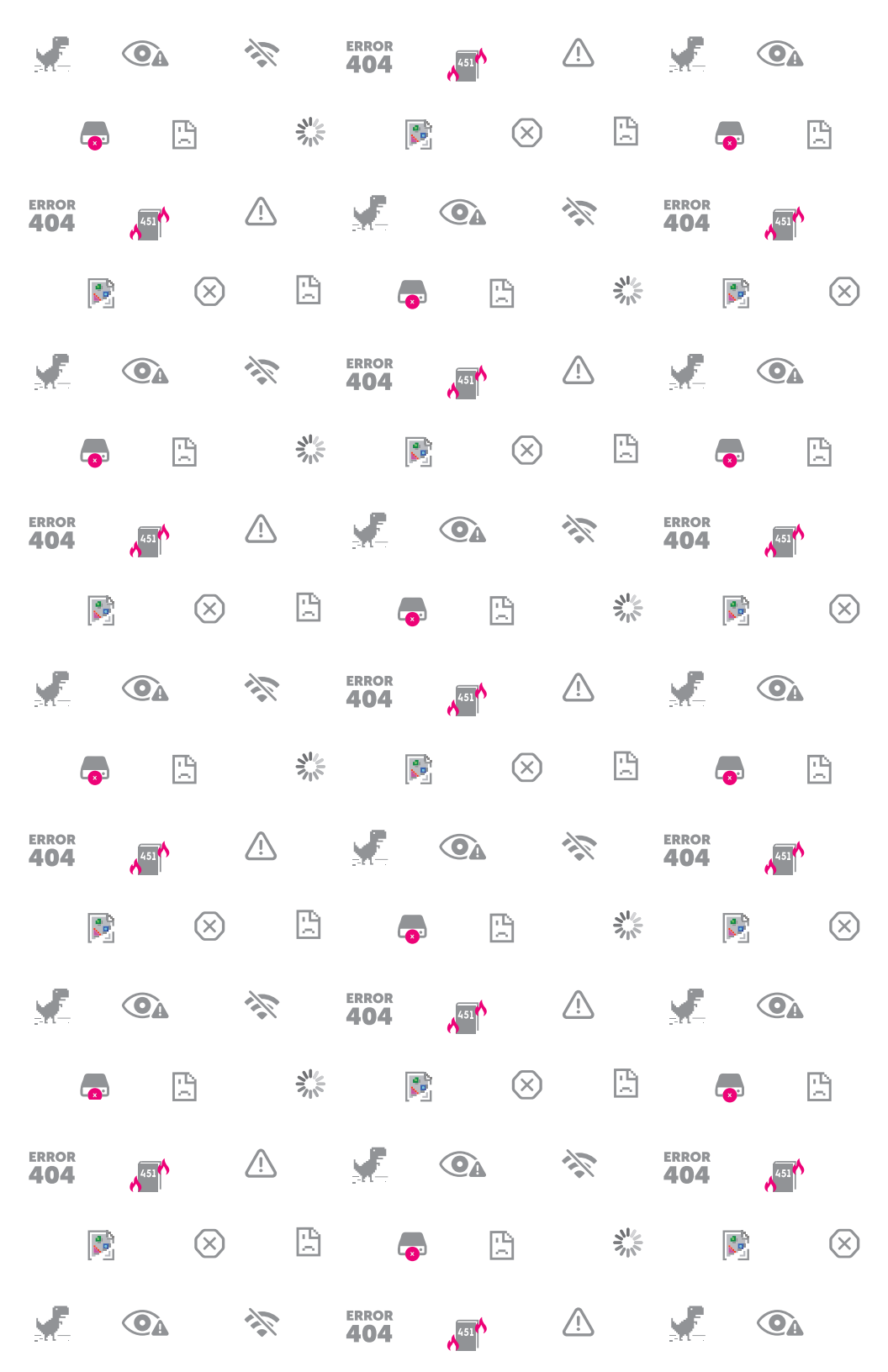


Gráfico de barras que muestra el número de incidentes de conectividad por estado durante el primer semestre de 2023, documentado por VE Sin Filtro.


ERROR
404
451

4 PROTECCIÓN DE DATOS PERSONALES Y SEGURIDAD DE SITIOS WEB DEL ESTADO

La protección de datos personales es fundamental para la seguridad y privacidad de los usuarios y ciudadanos. A medida que 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. Los datos en sí deben tratarse como una propiedad y las personas deben recibir una compensación justa por ellos[13].

Todo lo que hace una persona deja rastros digitales que pueden revelar detalles íntimos de sus pensamientos, creencias, movimientos, asociaciones y actividades[14]. 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[15].

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. 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.

> 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

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

a una actitud despreocupada de parte de los entes públicos y empresas privadas a hacer uso responsable de datos personales, cada ciudadano necesita tomar en sus propias manos la protección de la información sensible tanto como sea posible.

A pesar de cualquier esfuerzo, los Venezolanos siguen siendo altamente vulnerables a que sus datos sean expuestos, utilizados para fines inesperados, vendidos o accedidos por terceros. Las leyes y regulaciones vigentes fallan en los mecanismos para la protección de datos. No evitan su recolección, utilización o transferencia a terceros sin consentimiento. Tampoco responsabilizan a las organizaciones, públicas o privadas, por filtración de datos personales.

Como ejemplo, en julio de 2023, el Banco de Venezuela, el más grande del país, sufrió un ataque de ransomware a manos de la banda criminal Lockbit. Este incidente fue reportado por VE sin Filtro, basado en una publicación en el sitio web de la banda y otros canales de inteligencia digital. A pesar de la gravedad del ciberataque, inicialmente fue negado por el banco, que es de propiedad del Estado. Eventualmente, después de aparentemente optar por no pagar el rescate, una cantidad significativa de datos de los servidores fue publicada por Lockbit.

No pudimos encontrar esfuerzos por parte del banco para notificar o resarcir a las víctimas cuyos datos personales fueron expuestos. El foco de los datos expuestos estuvo principalmente en documentos internos y de algunos clientes corporativos. Si la violación hubiera incluido un rango más amplio de datos de clientes, el número de individuos afectados pudo haber sido mucho mayor. Este incidente subraya la vulnerabilidad de los sistemas digitales y la necesidad urgente de medidas robustas de ciberseguridad y protocolos de informes transparentes en caso de violaciones de datos.

4.1 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. Sus servidores deben ser seguros y los datos no ser accesibles para terceros; constatar que las contraseñas de los usuarios pueden mantenerse seguras; establecer protocolos de recuperación que no sean vulnerables al abuso y tomar medidas para que los usuarios de sus sistemas puedan saber que están en un sitio genuino, especialmente en un contexto donde muchos 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 méto-

dos 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/TLS

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 se sirven por HTTPS con certificado SSL/TLS firmado por una autoridad certificadora reconocida por los principales navegadores web, es decir la información transmitida y recibida por estas páginas se envía y recibe sin y no se puede verificar la autenticidad del servidor.

De esta lista, se identificaron 32 sitios con manejo de información sensible, de los cuales 30 tienen un inicio de sesión, 17 en los que solo se puede tener una cuenta si eres autorizado previamente por el administrador del mismo. Los 13 sitios restantes son páginas con login de uso público para realizar trámites fundamentales como la página del saime (siic.saime.gob.ve) que permite solicitar la cédula de identidad y el pasaporte. La mitad (6 de estos) no posee certificados SSL lo que quiere 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 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 pueden 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 se consultan los datos de los ciudadanos con su numero de cedula y fecha de nacimiento.

DOMINIO	ENTE PÚBLICO	SSL	2FA
petroapp.petro.gob.ve	Petroapp	Sí	Sí
bdvenlinea.banvenez.com	BDVenlínea	Sí	No
persona.patria.org.ve/login/clave	Monedero Patria	Sí	No
siic.saime.gob.ve	SAIME - Trámites	Sí	No
tramites.saren.gob.ve	TRAMITES EN LINEA SAREN	Sí	No
vicesocial.info	Vicesocial Venezuela. Consulta por Cédula ACTUALIZADO 2023	Sí	No
emprenderjuntos.gob.ve/autenticacion	Emprender Juntos	Sí	No
www.cne.gob.ve	Consejo Nacional Electoral	No	N/A
www.ivss.gov.ve	IVSS Instituto Venezolano de los Seguros Sociales	No	N/A
certificacioninternacional.mijp.gob.ve	Certificación de Antecedentes Penales	No	No
contribuyente.seniat.gob.ve/iseniatlogin/contribuyente.do	SENIAT - Servicio Integrado de Administración Aduanera y Tributaria	No	No
legalizacionve.mppre.gob.ve	Sistema de Legalización y Apostilla Electrónica	No	No
put.intt.gob.ve/login.php	Planilla Única de Trámites - INTT	No	No
webpi.sapi.gob.ve/indexo.php	WEBPI - Sistema En Línea de Propiedad Intelectual	No	No
www.imprentanacional.gob.ve/certificado_gaceta/site/	Sistema de Certificación de Gaceta	No	No
defensa-asegurado.sudeaseg.gob.ve	Sistema de Derechos y Defensa del Asegurado	Sí	LOGIN PRIV
fuerzalaboral.sudeaseg.gob.ve/ServidorFL/Proyectos/FuerzaLaboral/index.php	Fuerza Laboral	Sí	LOGIN PRIV
gsr.sudeaseg.gob.ve/login	SIS GSR	Sí	LOGIN PRIV
rton.sudeaseg.gob.ve/DPCLC_2/Proyectos/DPCLC_2/index.php	sudeaseg	Sí	LOGIN PRIV
sefam.sudeaseg.gob.ve/Servidor/Proyectos/EstadosFinancieros/index.php	SEFA Sistema de Estados Financieros Analíticos SEFA	Sí	LOGIN PRIV
tvl.sudeaseg.gob.ve/login	SUDEASEG | UsuariosExternos	Sí	LOGIN PRIV
uam.edu.ve	Universidad Arturo Michelena	Sí	LOGIN PRIV
virtual.uvm.edu.ve	Universidad Valle del Momboy	Sí	LOGIN PRIV
www.inscripciones.uc.edu.ve	Universidad de Carabobo - DICES	Sí	LOGIN PRIV
aulavirtual.ujap.edu.ve	Plataforma Acrópolis / Universidad José Antonio Páez	No	LOGIN PRIV
dgpatrimonios.seniat.gob.ve/auth	SENIAT	No	LOGIN PRIV
elegibilidad.banavih.gob.ve	BANAVIH	No	LOGIN PRIV

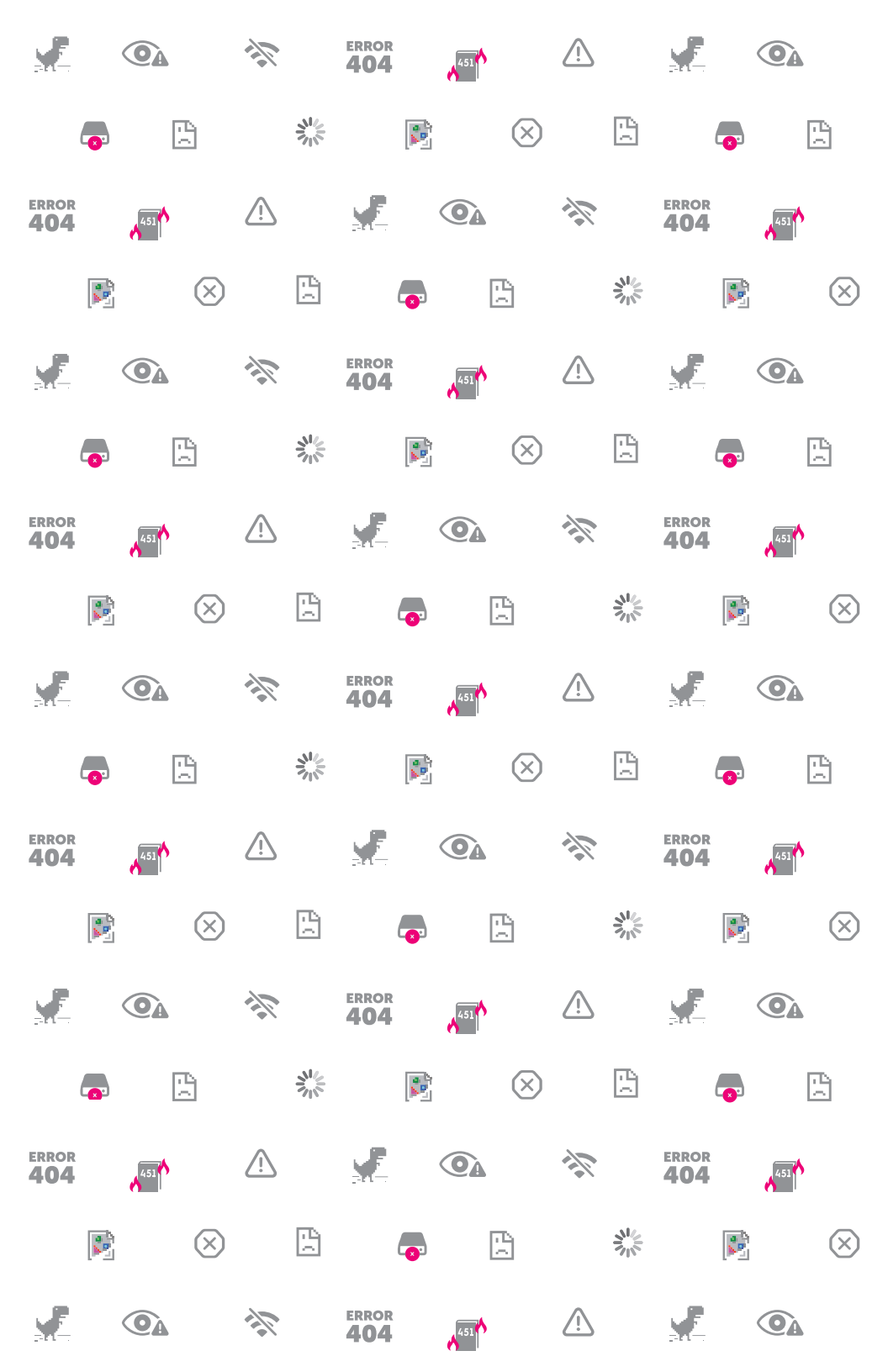
DOMINIO	ENTE PÚBLICO	SSL	2FA
faovel.banavih.gob.ve	FAOV	No	LOGIN PRIV
https://almccs.gob.ve/site/login.html	ALMACENADORA CARACAS	No	LOGIN PRIV
rncenlinea.snc.gob.ve	Sistema RNC	No	LOGIN PRIV
www.tsj.gob.ve	Tribunal Supremo de Justicia	No	LOGIN PRIV

Tabla listando una selección de sitios web del Estado, clasificados según disponibilidad de certificados SSL/TLS y de autenticación de múltiples factores. En sitios con login privado no se pudo verificar la disponibilidad de autenticación de múltiples factores.

Otro factor de seguridad importante es el proceso de recuperación o cambio de contraseña. El sitio del Seniat en línea, tiene una opción de recuperación de acceso antes de iniciar. La sesión llamada “Olvidó toda su información”, en la cual solicitan una combinación de preguntas fáciles de adivinar, datos personales públicos y otros que se podrían conseguir fácilmente.

Los métodos vulnerables de inicio de sesión o de recuperación de contraseña en los sitios web gubernamentales pueden exponer a las personas a muchas formas de abuso, incluyendo el robo de identidad y actividades maliciosas diseñadas para perjudicar la capacidad de los usuarios de solicitar asistencia gubernamental, dificultar la obtención de servicios e incluso dejarlos sin pasaportes válidos en un país donde puede tardar varios meses obtener uno.

Un número significativo de sitios web gubernamentales sí ofrecen un certificado SSL/TLS. Sin embargo, a diferencia de la mayoría de los sitios web genuinos donde el certificado está firmado por una autoridad de confianza, confirmando la autenticidad del servidor, estos sitios web a menudo usan certificados "auto-firmados". Esto provoca que el navegador web muestre una advertencia de que no puede verificar su autenticidad. Desafortunadamente, esto ha llevado a los usuarios a aprender a ignorar la advertencia y proceder, lo cual, bajo circunstancias normales, es un comportamiento riesgoso.


ERROR
404
451

5 FALTA DE ACCESIBILIDAD COMO LIMITACIÓN AL EJERCICIO DE DERECHOS EN INTERNET

Es imposible negar la importancia de Internet para la participación plena en la sociedad y el ejercicio de los derechos humanos. Sin embargo, las personas con discapacidad están seriamente desprotegidas porque abundan los portales oficiales y las fuentes de información que no cumplen 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, crea dificultades que hacen los sistemas más difíciles de usar para todo tipo de usuarios, especialmente aquellos con discapacidad.**

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 a las disponibles en dispositivos de consumo masivo. 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.

Reportes de la Confederación Sordos de Venezuela (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 sin 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.

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 manipulación de forma privada e independiente de otras personas.

El sitio web del Servicio Administrativo de Identificación, Migración y Extranjería, por ejemplo, publica los instructivos de cómo utilizar la página para distintos trámites con videos con audio sin subtítulos ni interpretación en lenguaje de señas y la página no puede ser navegada por medio del teclado.

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.

La página del 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.

6 ATAQUES DIGITALES

6.1 Phishing y robo de cuentas

En el pasado se ha 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 a 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[16] 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 residenciales a Internet, 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.

Aunque no se han documentado nuevas campañas de phishing a gran escala como estas, es una amenaza constante. El control sobre CANTV 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 que estañ disponibles en el whatsApp de las víctimas, permitiendo 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 inteligencia 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

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

motivación del ataque; o que ocurra sin interacción alguna de la víctima mediante la intercepción de mensajes o el cambio de SIM.

6.2 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.

Medios de comunicación independientes y organizaciones de la sociedad civil en Venezuela se enfrentan de forma cada vez más frecuente a falsas amenazas legales y el abuso, sin fundamentos de marcos regulatorios de protección de derechos de autor en otras jurisdicciones, para provocar la remoción de contenidos que les resultan incómodos a distintos actores

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.

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 especialmente graves 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. Tácticas como estas continúan siendo usadas por múltiples actores en 2022 y 2023.

6.3 Políticas de revisión de contenidos y su abuso

Las respuestas de las plataformas, especialmente las de Twitter y YouTube, a las sanciones y a la desinformación procedente de cuentas asociadas al Gobierno nacional 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 servicios en línea restringen el uso o acceso a sus servicios para los venezolanos, en un sobrecumplimiento de las sanciones que están obligados a acatar, dependiendo de la jurisdicción desde la cual operan. Muchas empresas internacionales de tecnología financiera han dejado de prestar servicios a clientes venezolanos, colocándolos en una situación aún más vulnerable.

Múltiples usuarios y medios independientes han visto sus cuentas de redes sociales sancionadas por violar las normas de plataformas sobre noticias falsas e imágenes violentas, al cubrir, documentar o comentar las declaraciones de funcionarios públicos u otros eventos. Muchas plataformas digitales distinguen entre el contenido sensible o dañino publicado por usuarios y las publicaciones que denuncian o documentan hechos, como en el caso de los medios, pero con frecuencia medios independientes de Venezuela acaban teniendo dificultades por la revisión del contenido.

Las plataformas deberían proactivamente publicar guías más claras diseñadas para periodistas y medios sobre cómo pueden documentar contenidos nocivos sin infringir las normas y qué hacer si el contenido es retirado injustamente.

6.4 Intimidaciones y amenazas

Continúa el uso de redes sociales y otras plataformas en línea para acosar a periodistas, organizaciones de la sociedad civil, activistas y medios. Con frecuencia estas acciones son especialmente agresivas contra periodistas, mujeres y otras comunidades marginadas que comparten opiniones.

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 todas 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.

A modo de ejemplo, 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

6.5 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.

DoS

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, incluyendo dispositivos propiedad del atacante, utilizando dispositivos de terceros comprometidos o incluso contratando el servicio de grupos delictivos.

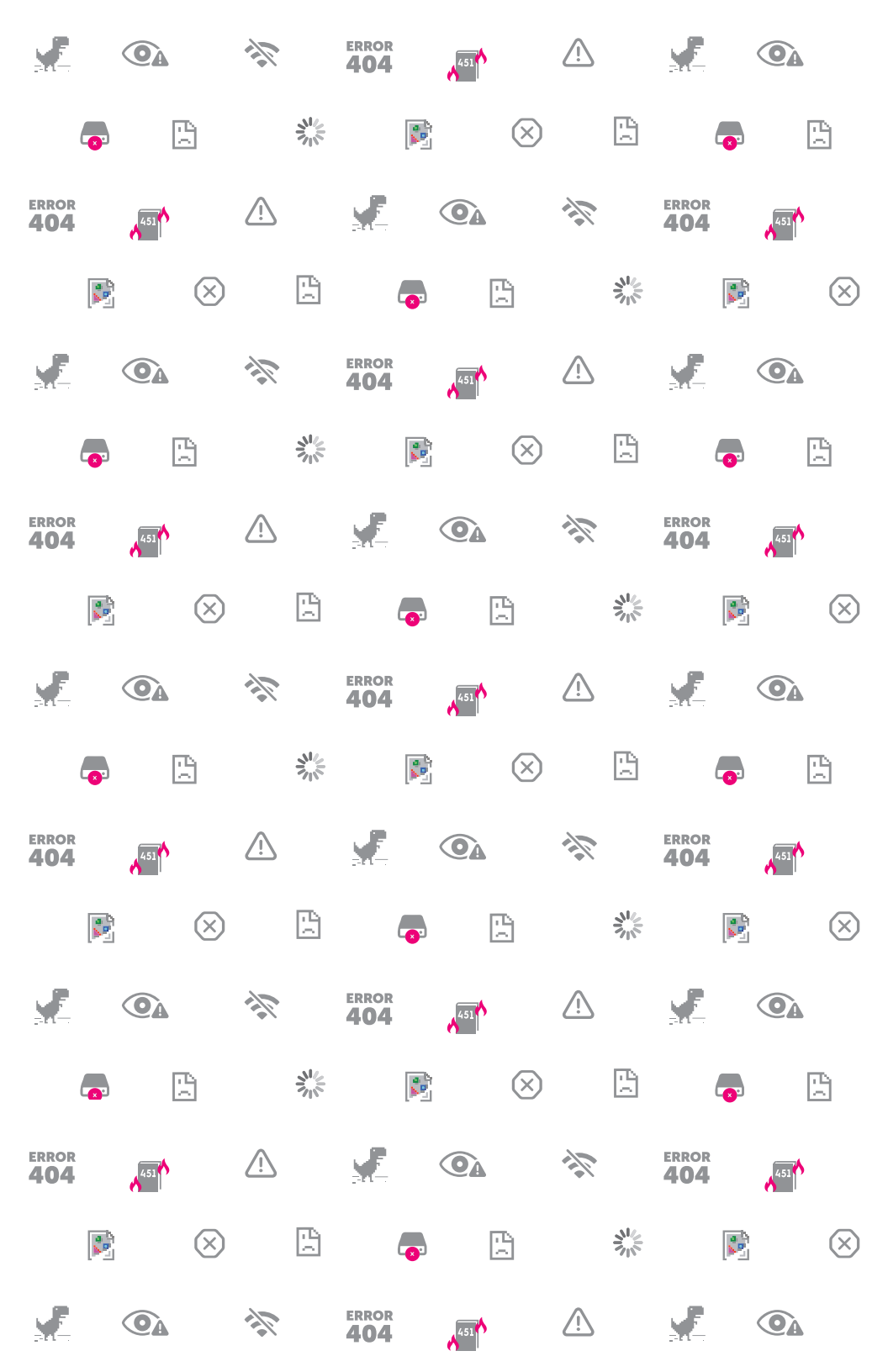
DDoS

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 inconveniente para el perpetrador.

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 podrían haber tenido acceso administrativo a los servidores web de su organización y sus datos. 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, no dirigidos. Los servidores desactualizados o mal configurados han sido un problema, como se ha observado en múltiples ocasiones por VE sin Filtro ilustrando las complejas vulnerabilidades y los recursos limitados de las organizaciones que trabajan en este contexto.


ERROR
404
451

7 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 presión.

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; no se debe esperar lo mismo de empresas que operan oficialmente en Venezuela ni en el creciente número de aplicaciones administradas por el Gobierno, en las cuales más bien se debe asumir que las autoridades pueden acceder a cualquier información en ellas, incluso información que pareciera ser privada.

7.1 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[17] 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[18] 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.

El domingo 13 de noviembre de 2022, el Cuerpo de Investigaciones Científicas, Penales y Criminalísticas (CICPC) informó que detuvo[19] 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[20] 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.

7.2 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, como presentamos en una publicación de Junio 2022. Estas intervenciones se habrían hecho por órdenes del gobierno de Nicolás Maduro en una violación masiva del derecho a la privacidad.

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

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

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

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

El informe de 2022 omitió todas las cifras de solicitudes del gobierno de Venezuela a la empresa. La opacidad en este informe de transparencia podría venir de presiones del Gobierno o el interés de Telefónica de manejar su reputación luego del impacto de las conclusiones de VE sin Filtro que contextualizan el informe de 2021, las cuales llegaron a noticias de Washington Post, El País e informes de las Naciones Unidas.

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 o.3% de las líneas en el peor de los casos.

Interceptaciones en 2021 según informe de Telefónica

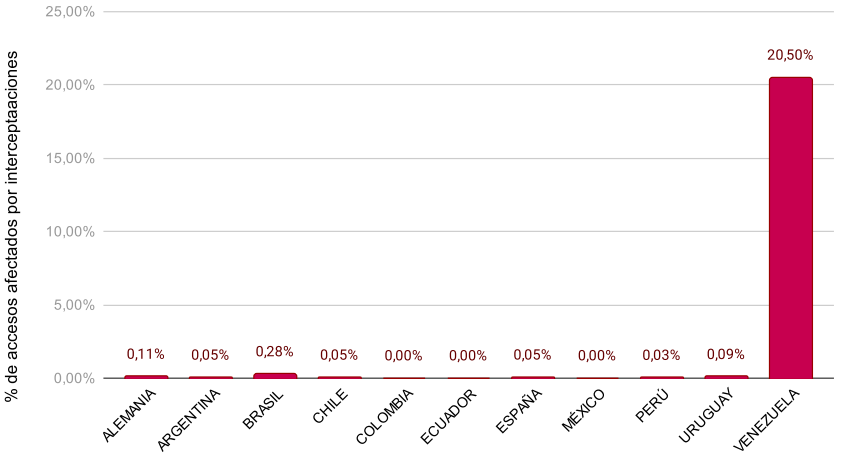


Gráfico de barras que muestra el porcentaje de líneas de clientes (accesos) de empresas filiales de Telefónica afectadas por interceptaciones de telecomunicaciones en distintos países. (Fuente: VE sin Filtro, utilizando datos de los reportes de transparencia de Telefónica)

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.

Adicionalmente, aunque no existen informes públicos que detallen el uso de spyware instalado en teléfonos móviles —lo que permitiría al gobierno espiar los contenidos de los dispositivos, y monitorear las comunicaciones y actividades de sus objetivos— algunos incidentes reportados por usuarios sugieren su uso a cierto nivel. Es altamente creíble que el gobierno venezolano tenga acceso y utilice tales herramientas.

Esto se alínea con su adquisición de herramientas de extracción de datos en dispositivos que controlan físicamente. Dado el contexto de abusos generalizados a los derechos humanos y los desmedidos poderes de vigilancia del gobierno, disidentes, periodistas investigativos y defensores de derechos humanos deberían considerar esto como una amenaza potencial sería.

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.

7.3 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.

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[21].

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 Diciembre de 2022, el municipio Chacao, en Caracas, lanzó 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 alcaldía de Chacao no dio respuesta a una solicitud de información pública de VE sin Filtro sobre las capacidades de reconocimiento

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

facial, protocolos de uso y su posible acceso en tiempo real por el gobierno nacional de su sistema de video vigilancia.

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[22], lo cual sugiere una cooperación más estrecha con las fuerzas de seguridad nacionales en situaciones políticamente sensibles de lo que muchos suponían.

Existen 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.

7.4 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 gobierno nacional 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 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.**

Hemos 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.

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

Adicionalmente, las autoridades venezolanas han adquirido unidades Cellebrite UFED Touch, 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 documentado múltiples casos de inspecciones del contenido de dispositivos personales durante interrogatorios irregulares a al menos seis miembros de diferentes organizaciones de la sociedad civil, al entrar o salir de Venezuela por aeropuertos internacionales, algunos de ellos fueron sometidos a esto varias veces.

Durante los interrogatorios, a las víctimas se les preguntaba sobre el contenido de sus dispositivos, y **a menudo eran coaccionadas para desbloquearlos y responder preguntas mientras los oficiales inspeccionaban documentos, contactos, comunicaciones y otros contenidos.**

En la mayoría de los casos, dispositivos con información sensible y personal también eran llevados a otra habitación, posiblemente para extracción de datos, en varios casos luego de haber sido desbloqueados en el interrogatorio. Esta preocupante tendencia coincide con una persecución aumentada contra la sociedad civil, y los actores cívicos deberían tomar precauciones.

8 METODOLOGÍA TÉCNICA

La documentación de los bloqueos y de los incidentes de conectividad se hace siguiendo estándares y criterios técnicos descritos a continuación.

8.1 Bloqueos de Internet

Entendemos un bloqueo de Internet **como una medida técnica deliberada con la intención de impedir acceso a una información, servicio o servidor en Internet,** interfiriendo en el comportamiento normal del tráfico. Esto ocurre intencionalmente con el propósito de censurar y controlar lo que los ciudadanos pueden hacer y ver en línea, mediante el uso de una o más medidas técnicas.

La implementación de eventos de bloqueo de contenido web puede tener distintas motivaciones.

En VE sin Filtro utilizamos el siguiente criterio para determinar que algo es un bloqueo en Internet:

- Identificable
- Medible
- Consistente
- Se entiende cómo opera el bloqueo y se pueden descartar otras explicaciones por el comportamiento.

Eventos de bloqueo: Los bloqueos son documentados principalmente como eventos, para evitar la ambigüedad que puede existir cuando distintas acciones de bloqueo afectan a un mismo servicio en Internet. El término evento de bloqueo hace referencia al bloqueo de una URL, dominio o dirección IP, utilizando una técnica de bloqueo específica y por un ISP en particular.

Por ejemplo: el URL "caraotadigital.xyz" perteneciente al sito web del medio de noticias Caraota Digital, presenta 7 eventos de bloqueos, estos son 6 bloqueos de tipo DNS en los ISPs CANTV, Digitel, Movistar, Inter, Net Uno y Supercable, y un bloqueo de tipo HTTP en CANTV, por lo que se registró un total de 7 eventos de bloqueo en un mismo caso.

Casos de Bloqueo: Todos los eventos de bloqueo contra un mismo servicio o sitio web se consideran un caso, que agrupa a los eventos de bloqueos contra distintos dominios, así como cada forma de censura implementada por los diferentes ISP.

Para medir la censura en Internet en Venezuela se realizaron mediciones de red estandarizadas de forma sistemática y mediciones de red manuales para confirmar algunos resultados. desde varios puntos de acceso en la red. Que son analizadas por VE sin Filtro y comparadas con otras mediciones y fuentes de información

La mayoría de las mediciones estandarizadas son realizadas con el software OONI Probe de OONI — pero no limitados a — que hemos utilizado para este reporte son:

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

La prueba de conectividad web de OONI está diseñada para medir si los sitios web están bloqueados mediante la manipulación de DNS, el bloqueo de TCP/IP o si se selecciona el tráfico a bloquear en base en detalles comunicados en los protocolos HTTP o HTTPS. Esta prueba se realiza automáticamente tanto sobre el punto de vista del usuario como desde un punto de vista de control no censurado. Si los resultados de ambos puntos de vista coinciden, lo más probable es que se pueda acceder al sitio web probado. Sin embargo, si los resultados difieren, la medición se marca como anómala.

Para monitorear la accesibilidad de las plataformas populares de mensajería instantánea a lo largo del tiempo, realizamos las pruebas de WhatsApp, Facebook Messenger y Telegram de OONI.

Monitoreamos la accesibilidad y el funcionamiento de las herramientas de evasión de la censura mediante una mezcla de técnicas. Comprobamos el funcionamiento de una lista de VPNs y otras herramientas anti-censura manualmente, medimos el acceso a sitios de herramientas anti-censurase es a través de la prueba de conectividad web de OONI, y también realizamos pruebas de OONI para herramientas específicas, especialmente Tor.

8.2 Conectividad

El análisis técnico de los niveles de conectividad, tanto en tiempo real como posterior, se realiza principalmente utilizando sistemas propios y que consultan datos de IODA (Internet Outage Detection and Analysis, por sus siglas en inglés) y del Instituto Tecnológico de Georgia, que genera un historial de los datos de conectividad a nivel mundial.

Esta data obtenida mediante el API de IODA, es procesada y analizada para identificar las caídas de conectividad a nivel nacional, y a su vez se realiza un trabajo de investigación para determinar el origen de las caídas

de conectividad. La data de IODA se complementa con consultas en Cloudflare Radar y Google Traffic Transparency report.

Una caída de conectividad es definida como un incidente, el cual influye de forma diferente en cada estado del país, por lo que se define como un evento cada caída regional o en un ISP en particular producidas por un incidente específico.

Con respecto al criterio de identificación de los incidentes/eventos, se establecieron dos clasificaciones donde cae la conectividad a Internet:

1. Magnitud de la caída de los niveles de conectividad:
    - a Crítica: si está entre 0% y 50%
    - b Seria: si está entre 50% y 80%
    - c Leve: si se observa una caída que no es inferior a 80%, y a su vez coincide con un evento evidente de baja de conectividad. No se refiere a variaciones normales.
2. Causa del incidente:
    - a Por fallas eléctricas
    - b Por falla de proveedores de Internet
    - c otras

La principal señal utilizada para evaluar la gravedad de estos incidentes es la conectividad medida por IODA como el sondeo activo de direcciones IP desde Internet, contando el número de pequeños segmentos de direcciones IP (segmentos de red /24) que consideran conectados a Internet si las direcciones de del segmento pudieron ser contactadas. Es importante conocer que las mediciones tienen como métrica segmentos de red /24 normalizados con respecto al valor más alto de conectividad de la región o ISP, que se está monitoreando.

El objetivo principal de este proceso es identificar caídas de conectividad de gran magnitud (macroscópicos), que afecten significativamente al país y/o una región y/o a un proveedor del servicio de Internet en Venezuela.

ANEXO

Sitios bloqueados en 2022 y 2023

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

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

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

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

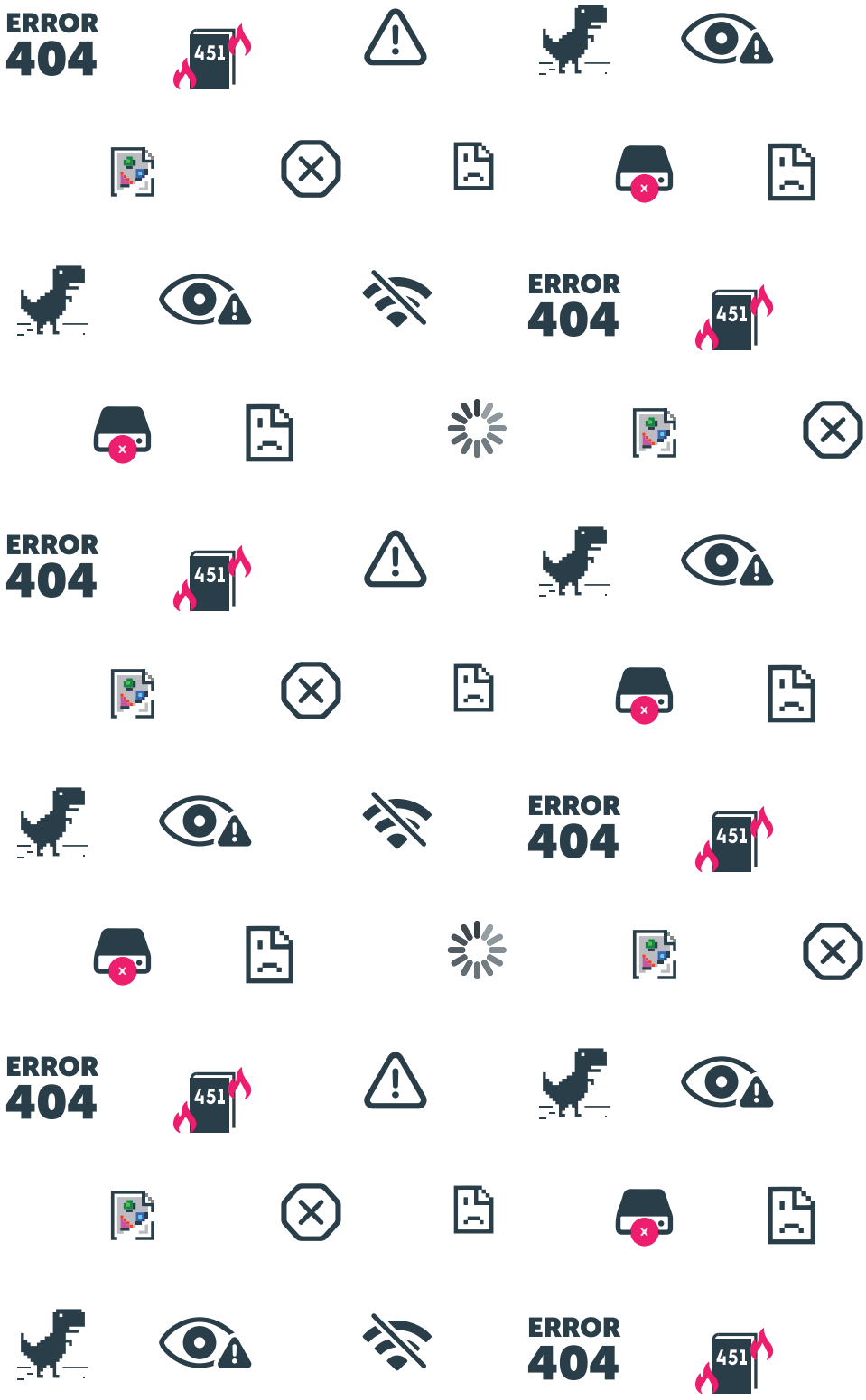
runrun.es	Runrunes	NEWS	DNS	DNS	No	No	No	No	No	No	DNS	DNS	No	No
sumarium.es	Sumarium	NEWS	HTTP/HTTPS	DNS + HTTPS	No	No	No	No	No	No	No	No	No	No
www.tvvenezuela.tv	TV Venezuela	NEWS	DNS	DNS	DNS	DNS	DNS	DNS	DNS	DNS	DNS	DNS	DNS	DNS
venezuelaaldia.com	Venezuela al dia	NEWS	No	No	DNS	DNS	No	No	DNS	DNS	DNS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

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

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

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

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


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